AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

[H.A.S.C. No. 113–13]

# NUCLEAR SECURITY: ACTIONS, ACCOUNTABILITY AND REFORM

HEARING

BEFORE THE

SUBCOMMITTEE ON STRATEGIC FORCES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

HEARING HELD
FEBRUARY 28, 2013

U.S. GOVERNMENT PRINTING OFFICE
79–996 WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office,
http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202–512–1800, or 866–512–1800 (toll-free). E-mail, gpo@custhelp.com.

SUBCOMMITTEE ON STRATEGIC FORCES

MIKE ROGERS, Alabama, *Chairman*

TRENT FRANKS, Arizona
DOUG LAMBORN, Colorado
MIKE COFFMAN, Colorado
MO BROOKS, Alabama
JOE WILSON, South Carolina
MICHAEL R. TURNER, Ohio
JOHN FLEMING, Louisiana
RICHARD B. NUGENT, Florida
JIM BRIDENSTINE, Oklahoma

JIM COOPER, Tennessee
LORETTA SANCHEZ, California
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JOHN GARAMENDI, California
HENRY C. "HANK" JOHNSON, JR., Georgia
ANDRÉ CARSON, Indiana
MARC A. VEASEY, Texas

DREW WALTER, *Professional Staff Member*
LEONOR TOMERO, *Counsel*
ERIC SMITH, *Clerk*

# CONTENTS

## CHRONOLOGICAL LIST OF HEARINGS

2013


Page

HEARING:

Thursday, February 28, 2013, Nuclear Security: Actions, Accountability and Reform ..... 1

APPENDIX:

Thursday, February 28, 2013 ..... 33


**THURSDAY, FEBRUARY 28, 2013**

**NUCLEAR SECURITY: ACTIONS, ACCOUNTABILITY AND REFORM**

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS


Cooper, Hon. Jim, a Representative from Tennessee, Ranking Member, Subcommittee on Strategic Forces ..... 3

Rogers, Hon. Mike, a Representative from Alabama, Chairman, Subcommittee on Strategic Forces ..... 1


WITNESSES


Alston, Maj Gen C. Donald, USAF (Ret.), Former Commander, 20th Air Force, Former Air Force Assistant Chief of Staff for Strategic Deterrence and Nuclear Integration; Brig Gen Sandra E. Finan, USAF, Commander, Air Force Nuclear Weapons Center, Former Principal Assistant Deputy Administrator for Military Applications, National Nuclear Security Administration; and Hon. Gregory H. Friedman, Inspector General, U.S. Department of Energy ..... 3

Poneman, Hon. Daniel B., Deputy Secretary of Energy, U.S. Department of Energy; and Hon. Neile L. Miller, Acting Administrator and Principal Deputy Administrator, National Nuclear Security Administration ..... 13


APPENDIX


PREPARED STATEMENTS:

Alston, Maj. Gen. C. Donald (Ret.) ..... 44
Cooper, Hon. Jim ..... 41
Finan, Brig Gen Sandra E. ..... 72
Friedman, Hon. Gregory H. ..... 91
Poneman, Hon. Daniel B. ..... 101
Rogers, Hon. Mike ..... 37

DOCUMENTS SUBMITTED FOR THE RECORD:

DOE Verbal Shortcuts and Acronyms ..... 111
NNSA Key Personnel ..... 112
DOE Organization Chart ..... 113
NNSA Organization Chart ..... 114

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:

Mr. Cooper ..... 117
Mr. Garamendi ..... 117

Page

QUESTIONS SUBMITTED BY MEMBERS POST HEARING:
Mr. Cooper ..... 139
Mr. Rogers ..... 121

# NUCLEAR SECURITY: ACTIONS, ACCOUNTABILITY AND REFORM

---

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON STRATEGIC FORCES,
*Washington, DC, Thursday, February 28, 2013.*

The subcommittee met, pursuant to call, at 10:30 a.m., in room 2212, Rayburn House Office Building, Hon. Mike Rogers (chairman of the subcommittee) presiding.

## OPENING STATEMENT OF HON. MIKE ROGERS, A REPRESENTATIVE FROM ALABAMA, CHAIRMAN, SUBCOMMITTEE ON STRATEGIC FORCES

Mr. ROGERS. This hearing of the Armed Services Subcommittee on Strategic Forces is called to order. I want to say good morning and welcome everybody to today's hearing on nuclear security at the Department of Energy's National Nuclear Security Administration [NNSA]. Before we get into the hearing, I want to welcome our new members to the committee. First and foremost, I want to recognize our ranking member, Mr. Cooper of Tennessee, my friend and colleague of many years. I look forward to working closely with him over the next 2 years as we carry out this important work.

I am not sure they are here, but new to our Strategic Forces Subcommittee on the Republican side are Mr. Coffman of Colorado, Mr. Wilson of South Carolina, Mr. Nugent of Florida, Mr. Bridenstine of Oklahoma. On the Democrat side: Mr. Johnson of Georgia, and Mr. Carson of Indiana, and Mr. Veasey of Texas. I look forward to working with all of you, as well as my colleagues who are returning for another 2 years on the Strategic Forces oversight subcommittee.

This subcommittee has responsibility for many big critical important issues, and we are going to get into one of them right now. Today's hearing is part of the committee's continuing oversight of the aftermath of the security breach at Y–12 National Security Complex in July of last year. At this point, the facts of the incident are well established so I won't repeat them. Needless to say, the intrusion was astonishing and completely unacceptable.

Through its hearing and closed briefing last September, the subcommittee is aware of the immediate corrective actions taken by the NNSA and the DOE [Department of Energy]. Today's hearing is focused on the broader implications of the incident, including organizational leadership and structural failures that enabled it to occur. Reviewing the testimony from our first witness panel as well as the other reports on DOE nuclear security stretching back 15 years, I am deeply concerned that we have been identifying the same problem for more than a decade.

For instance, in a 1999 report by the President's Foreign Intelligence Advisory Board, it said the DOE, "Embodied science at its very best and security at its worst."

Highlighting a string of recurring security problems in the 1990s, the board described DOE as a "dysfunctional bureaucracy that has proven it is incapable of reforming itself."

In 2002, a few years after Congress created NNSA in an effort to address these concerns, another study by the Commission on Science and Security found the same problems. In 2005, an independent study of NNSA security conducted by Admiral Richard Mies again made very similar findings saying that the problems were, "they are not new, many continue to exist because of the lack of clear accountability, excessive bureaucracy, and organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes."

Those reports were from 1999, 2002 and 2005. So where are we today? To anyone paying attention, the answer is undeniably, nowhere. The assessments done after the Y–12 incident showed that the exact same fundamental problems remain. Regardless of the structural issues, there is also a problem of accountability. The only people who have been fired as a result of the Y–12 incident are a few guards, but no Federal officials have been fired. Some NNSA site and headquarters security officials have been reassigned to other positions within the DOD or allowed to retire but not fired. This is not accountability. It is the exact opposite of what Secretary of Defense Gates did after the Air Force's nuclear security problems in 2007 and 2008. His demonstration of accountability in the Air Force's senior-most leadership is my example of a firm system of accountability, and it should be everyone's.

Our first panel of witnesses will help us explore what changes are needed to ensure a breach like Y–12 does not happen again. They are each the author of separate independent assessments of the Y–12 incident or broader security issues at DOD and NNSA. The witnesses are Major General Donald Alston, former commander, 20th Air Force, and former Air Force Assistant Chief of Staff, Strategic Deterrence and Nuclear Integration; Brigadier General Sandra Finan, U.S. Air Force, Commander of the Air Force Nuclear Weapons Center, and former Principal Deputy Assistant Administrator for Military Applications, National Nuclear Security Administration; and the Honorable Gregory Friedman, Inspector General, U.S. Department of Energy. I want to thank our witnesses for appearing today and the time they have put in preparing their testimony. I know it is a labor, but we do appreciate it.

I have a longer version of my statement that I am, without objection, going to offer for the record. Hearing none, it is so ordered. And with that, I want to turn to my friend and colleague from Tennessee, Mr. Jim Cooper, for any opening comments that he may have.

[The prepared statement of Mr. Rogers can be found in the Appendix on page 37.]

**STATEMENT OF HON. JIM COOPER, A REPRESENTATIVE FROM TENNESSEE, RANKING MEMBER, SUBCOMMITTEE ON STRATEGIC FORCES**

Mr. COOPER. Thank you, Chairman Rogers, I look forward to working with you and our colleagues on these important issues this year. I would just like to ask, in view of the shortness of the time, that my opening statement be inserted in the record.

[The prepared statement of Mr. Cooper can be found in the Appendix on page 41.]

Mr. ROGERS. Thank you, sir. In concert with that, as you all may have been told before the hearing we will be called for votes in a little while, so we will dispense with the reading of your opening statements; they will be submitted for the record without objection, and we will go straight to the questioning of the witnesses. The witness order will be General Alston, sorry, we won't let you stay retired; General Finan, thanks for putting your NNSA hat on one last time to help the subcommittee understand these issues, and Mr. Friedman.

[The prepared statements of General Alston, General Finan, and Mr. Friedman can be found in the Appendix beginning on page 44.]

**MAJ GEN C. DONALD ALSTON, USAF (RET.), FORMER COMMANDER, 20TH AIR FORCE, FORMER AIR FORCE ASSISTANT CHIEF OF STAFF FOR STRATEGIC DETERRENCE AND NUCLEAR INTEGRATION; BRIG GEN SANDRA E. FINAN, USAF, COMMANDER, AIR FORCE NUCLEAR WEAPONS CENTER, FORMER PRINCIPAL ASSISTANT DEPUTY ADMINISTRATOR FOR MILITARY APPLICATIONS, NATIONAL NUCLEAR SECURITY ADMINISTRATION; AND HON. GREGORY H. FRIEDMAN, INSPECTOR GENERAL, U.S. DEPARTMENT OF ENERGY**

Mr. ROGERS. We will begin with 5-minute rounds of questions and then we will have a second panel after that. I will start the questions here.

General Alston, you and Mr. Augustine and Dr. Meserve seem to have read the many reports and independent reviews of DOE security that have been conducted previously. Your letter to Secretary Chu calls it, "The considerable body of work that has been done on the subject over the past decade." In particular, you mention the review done by Admiral Mies in 2005. You heard me, in my opening statement, mention a few others, but there are many more. How do your findings and recommendations compare to those contained in the findings of all the previous reports?

General ALSTON. Mr. Chairman, thank you very much.

Mr. ROGERS. Your microphone needs to be turned on, please.

General ALSTON. Need coaching and I am trainable. Mr. Chairman, thank you for the question, I would say that probably the most disturbing thing that Dr. Meserve, Mr. Augustine, and I found was the recurring evidence of problems that have existed before. And when you take a close look at Admiral Mies' work that he did, I count about 111 recommendations that the Department of Energy showed us, a matrix, we had grades on them, and without doing an exhaustive detailed cross-check of what Admiral Mies found and what we were finding but doing a rather cursory look

at that, I would take issue with a variety of those assessments in terms of the health of those particular findings.

Of course, since 2005, there has been a lot of time over the course of those 8 years, and I can't say that I saw any evidence of reaching back to the Mies reports. So I don't know how fresh the management of the Mies findings and recommendations was. I don't know the last time they revisited that or if that is a regular phenomenon that they do revisit all those findings. But just a few of them that point towards culture and things that we found to be a legacy of challenges in the Department of Energy: no team approach toward security, struggling to succeed in an atmosphere of conflicting viewpoints, headquarters versus the field, lab versus lab, site office versus contractor, academic versus operational, union versus management, and then non-NNSA elements in the Department of Energy.

There have been recurring challenges as site field offices would see a need to upgrade security. We saw lack of discipline, that Admiral Mies found as well, in terms of having a broad strategic vision for what the overall security requirements and standards should be, and a sensitivity to elevate the unique features of each site as opposed to having standardized common security requirements being the principal focus and the site offices having to defend wanting to be different. But without discipline and strong central management of that, then folks could conceive, design, develop, and deploy systems that might not be as fully vetted and ready as they need to be, and I think Y–12 is a good example of that.

Mr. ROGERS. Why do you think this culture was allowed to continue? Because it did happen over years. In your opinion, after each of these studies, were there any consequences and then they would lapse back into this culture or were there never any consequences?

General ALSTON. We found it difficult to have traceable authority from the field up the chain of command to find unambiguous certainty that somebody was in charge of one element of security or another. And because that seemed ambiguous, and because there was a prevailing notion that it is an eyes-on/hands-off surveillance mantra, that the field—the sites have, over time, enjoyed being distanced from the headquarters and sort of being alone and unafraid, and certainly, I was in a military organization and we didn't like interference from the headquarters.

However, when it comes to security, I think there are benefits to having good central management that may not be true for science, but I do believe it is true for security.

Mr. ROGERS. Do you believe that if there had been somebody at the top of the command chain held responsible for the findings of any of these earlier studies in a significant way by termination that it would have helped to eliminate that culture's continuance?

General ALSTON. Well, sir, that would be one action that could be taken, but that action alone I don't think would necessarily have resulted in all of the fundamental changes that would have had to occur.

Mr. ROGERS. Why?

General ALSTON. Well, I think that gets everybody's attention. I showed up on the Air Staff the same weekend that we had our unauthorized munitions transfer from Minot to Barksdale, a very epic

failure for our Air Force. So, I was there for the next 3 years working that particular problem. The Air Force did not—we worked the problem hard for the first year, but when we lost the Chief and the Secretary, life was different, and the entire Air Force had to rally around not a security problem, but an enterprise failure. And because we looked at this in the largest context, I believe that after spending 9 months working the problem to no one's satisfaction, that it certainly was an extraordinary accountability action by Secretary Gates which had the Air Force focus on that problem in a way that we had failed to focus on it before, this is absolutely true.

Mr. ROGERS. Thank you very much. The chair now recognizes the ranking member for any questions he may have.

Mr. COOPER. Thank you, Mr. Chairman. There are lots of issues here, too much red tape in the bureaucracy, questionable contractor performance. But I think that one thing folks back home understand is what do we get for taxpayer dollars? And the inspector general [IG] pointed out that DOE-wide we are spending something like $1 billion a year just in protection of facilities. And he mentions in his testimony that $700 million per year spent on complex-wide protective force of about 4,000 workers, contract professionals; that would be $175,000 compensation for each guard; that is a lot. And a lot of folks back home would ask, well, we paid all these people, did we get any security and result in return?

The focus, of course, of today's hearing is the Y–12 facility, which we discover now wasn't even nun-proofed, much less terrorist-proofed. And the expenditures are called for the Y–12 facility, we just spent $150 million a year protecting that one plant, and yet we couldn't catch two 70-year-olds and one 80-year-old as they breached the perimeter. And as the chairman has quite correctly pointed out, it is hard to find that anybody was punished except the lowest level guard, and it doesn't seem like this is a fair way to treat a security lapse of this type.

So I know that time is of the essence, I just want to encourage the IG and I appreciate the work of Meserve and Finan to help us understand this. But the bottom line is taxpayers need to get results for their dollars. Right now in DOE, it doesn't seem like we are getting those results. Welcome a comment, but I know that time is short.

Mr. FRIEDMAN. Mr. Cooper, are you asking me for a comment? I think you have synthesized the high points, several of the high points in our reports over time. I might point out that safeguards and security, from our perspective, has been a management challenge at the Department of Energy for at least the last decade, so this is a continuing problem. And if I may respond subsequently to a question from the chairman to General Alston, we have found over time that, I think the chairman phrased it exactly correctly, that there has been a lack of sustained effort to cure a problem. There has been sort of a short-term fix and then the fix, and the effort to fix evaporates over time.

And secondly, if I can, security cannot be a sideline, it has got to be integrated into the very essence of a production plant like Y–12 and all the other department facilities. So it has to be an integrated approach from the get-go to the end rather than a separate function. So I think those are two highlights, and your issue that

you have highlighted, Mr. Cooper, about costs are ones of course that concern us a great deal.

Mr. COOPER. It shouldn't just concern us. We paid no telling how many tens of hundreds, millions of dollars for cameras at Y–12 that didn't work, and an alarm system that gave off hundreds of false alarms a day. Where is the refund from the contractor? You know, the best we can tell, people got performance bonuses. Excellent ratings. This is astonishing that the taxpayer got back so little for their money, especially in such a secure installation. I thank the chairman; I yield back the balance of my time.

Mr. ROGERS. I thank the gentleman. The chair now recognizes my friend from Arizona, Mr. Franks, for 5 minutes.

Mr. FRANKS. Well, thank you, Mr. Chairman, thank all of you for being here. I don't want to mischaracterize my friend's comments about the 80-year-old nun, it seemed like he kind of did that in a rather diminishing way. I understand she was quite spry for 80, and that that should be taken into account. When you make the comparison about the guards costing about $175,000 a year for taxpayers, I have been looking at the numbers here, and that is about what Congress gets paid, and I am afraid the connections and the parallels here are a little frightening for someone like myself, because we wonder if maybe we are not all a little bit overpaid.

It is very easy for us to kind of, as I just did, make little jokes about these kinds of things and sort of step back from almost a holier-than-thou position. It is easy from an armchair perspective to say "how could this ever happen." And yet in a sense, that is a little bit—that is our job here on the committee to try to exert some oversight that hopefully will change a culture that has made a particular error here in a better direction.

I know that if we really were all honest with ourselves, we would look at this from a much larger perspective. History has been pretty unkind to those who have tried to maintain nuclear security. If we had done that well decades ago when we first gained this technology, the Soviets would never have gained that technology and there never would have been a Cold War. So, this is not as unprecedented; I think I remember some story where we had to drop one of our atomic bombs off the coast out of a plane, I think it is still there, years ago.

These are not as unprecedented as they seem, but because they are so serious, it occurs to me that we have to try to back up and ask ourselves, why is it that there is this hallmark for us letting these kinds of things be so easily secured when the implications are so profound? So I guess I am going to ask sort of a question for all of the panel members. If there was one thing that you could do in this particular instance and in a broader instance of trying to help both our civilians infrastructure and our military apparatus understand the need for more security when it comes to nuclear technology and weapons that have these profound implications, what is the one thing, General, I will start with you, that you would suggest that we do? Is it a mind-set? Is it a systemic issue? What would you postulate?

General ALSTON. Well, sir, I would tell you that Mr. Augustine and I, in particular, and I think Dr. Meserve mentioned it as well, but the cultural challenges facing the Department of Energy when

it comes to a culture that doesn't segment security, doesn't segment safety, but rather looks at them as all essential to mission as opposed to trade space, that that is a very profound challenge because taking culture on head-on is a very challenging effort. But, we found that this, and I have had recent discussions informally with people not involved directly with this where security is now perceived as, you know, we have to go through the hurt right now. And, security is perceived as sapping strength and competing with science and other priorities in the Department.

So I think there is still a long way to go in a pervasive culture where every last person that is working in NNSA or the Department of Energy sees security, and safety, and mission, not as separate things that need to be tended to, and prioritized, but rather have a common view how important and vital they are and essential every day to mission success.

Mr. FRANKS. General Finan.

General FINAN. Well, I would echo what General Alston just said and I think that is the primary thing you have to do is work on the culture so rather than repeat that, I think given culture as an issue that must be addressed, I think the next thing that we have to think about is lines of authority. We have to be very clear on who is responsible for what. We have to then follow up and give the authorities necessary to execute those responsibilities and once we do those two things throughout the chain of command, then we can hold people accountable. But one of the continuing things that NNSA and DOE before it have struggled with was defining roles and responsibilities and then giving the appropriate authority to execute those responsibilities, and that has been a longstanding issue that we really need to straighten out in order to create that accountability and ownership of that security mission.

Mr. FRIEDMAN. Mr. Franks, I concur with what has been said previously. And maybe this is too far down in the weeds, but if there was, in addition to what has already been said, if there was one problem, and I guess it builds on what General Finan just referred to is that we need to be sure that employees at all levels are empowered to raise serious issues and that there is a process in place to ensure that those issues are, in fact, addressed. I think that applies in terms of safety, it certainly applies in terms of security. And it certainly was a problem, a root cause problem we found at least with regard to the Y–12 issue and security generally throughout the Department of Energy.

Mr. FRANKS. Thank you. And thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman. The chair now recognizes Mr. Garamendi for 5 minutes.

Mr. GARAMENDI. I would like each of the witnesses to take a minute and a half and talk about where we are today. This is all history; what has been done along the lines, if you know, to carry out the recommendations that have been made? We will start with the General, General Finan.

General FINAN. I left NNSA over a month ago, but before I left, I can tell you that there was structural changes occurring within the security organization so they were in the process of implementing the recommendations to stand up an operationally focused organization that would help ensure standardization across the

fields. They were also in the process of creating standards and criteria for security so that people in the field would know what standard they needed to meet and what criteria would be used to evaluate them. There were personnel changes that had occurred in order to bring in what I call true security expertise. Security is a special skill, and we have people throughout this country who have those skills, and so we need to seek out those individuals and bring them in so that they can bring that skill set to the NNSA. So, that was ongoing. So, basically all the recommendations that I had out of my reports were being enacted at the time I left.

Mr. GARAMENDI. And Mr. Friedman.

Mr. FRIEDMAN. With regard to the recommendations we made in our earlier report, Congressman, we have not received the final departmental position, so we are not—we have heard anecdotal information of what steps have been taken and we are waiting for that to occur. In the interim, between our reports, both General Alston and his group and General Finan have done their reports. We have also issued a report on the contractor assurance system which is a system that NNSA has in place to evaluate contractor actions. We intend to go back at some point in the future and look at the process and determine whether the fixes that have been committed to and promised have, in fact, been made.

Mr. GARAMENDI. When is that point in the future?

Mr. FRIEDMAN. I guess that is the pointed question I wasn't prepared to answer. We will—it is a high priority for us because obviously security is essential in a nuclear weapons environment.

General ALSTON. I left the effort the first week of December, and the draft recommendations, which we were exposed to, were not in the charter that Secretary Chu had given us, so I don't think I am in a position to comment.

Mr. GARAMENDI. Good. Let me go back to you, Mr. Friedman. One of the oversight and review organizations is you, and it would seem to me that holding people accountable is what you guys do, so I am concerned about your response that at some point in the future and so on and so forth. I would like a more precise answer. And with that, Mr. Chairman, I yield back.

[The information referred to was not available at the time of printing.]

Mr. ROGERS. I thank the gentleman. The chair now recognizes Mr. Nugent for 5 minutes.

Mr. NUGENT. Mr. Friedman, just to follow up on Mr. Garamendi's question, you do the inspection, you prepare a report, you send it to the powers to be, and they are the ones that have to make things accountable, am I correct on that? Do you hold them accountable, or do the administrators hold their rank and file accountable?

Mr. FRIEDMAN. Well, our reports in these instances, Congressman, were sent to the Secretary; it is ultimately the Secretary's responsibility to hold his subordinates responsible.

Mr. NUGENT. I would think, General Alston, when you took over as related to the incident in the Air Force, were people held accountable at the upper echelons, or was it just the lowest ranking folks that are easy picking when something goes wrong, or do you

look at the culture, which I have heard from all three of you in regards to how things actually occur?

General ALSTON. Initially, it was just the lower level leadership, wing commander, squadron commander, a couple of group commanders, so there were a handful of colonels. Following the installation of the new Secretary and the new chief of staff, I know there was a further detailed review, and I am not privy to exactly what the actions were.

From a distance I understand that General Schwartz, as one of his initial responsibilities after evaluating how to do accountability in these circumstances, taking in stock not just the unauthorized movement in the nuclear weapons, but also the incident that involved some components that were opened in a box in Taiwan, that the chief of staff then personally dealt with the general officers in ways that I am just not personally privy to.

Mr. NUGENT. You know, in experience, in regards to leading an organization, somebody has to be accountable. And typically, when you discipline the lower ranks and you mentioned it, there are other folks because it is a culture, and all three of you have mentioned that, a culture of really failed leadership within NNSA and DOE as it relates to security. How do we—if you were in charge, how do you fix that specifically from the IG's perspective? Where does the ball finally end?

Mr. FRIEDMAN. As I alluded to in my earlier comment, Congressman, security cannot be treated as a stepchild, as a side show, it has got to be integrated into the process from the very outset. And that is one of the key issues that we have found has not been in place. You can call that a cultural issue, perhaps that is correct, and I think—I would refer to it as a "tone at the top" issue. It has to flow down from the highest levels of the Department and permeate and people have to be held accountable. I know that may sound like a textbook sort of lessons, but I think that is what needs to be done and it seems to me there has been a commitment to begin that process. And as I alluded to earlier, sustainability is really the issue. We are on a path now, we have anecdotal information that changes have been made, not personnel changes that you are referring to, I understand that, but changes have been made in the systems. The question is will that be sustained going forward?

Mr. NUGENT. And it really is buy-in from the leadership. You can change systems and you can change policies, but if there is no one there to actually make sure that the rank and file are following the policies and procedures, nothing gets done from a positive standpoint. So we can talk the game, but at the end of the day how is NNSA and DOE actually going to hold the upper-level administrators accountable for the security that is so important to this Nation? How do you suggest that happen?

Mr. FRIEDMAN. Well, I think the administrator of NNSA reports to the Secretary of Energy under the current format. And ultimately, and obviously there are changes in process as we speak. Ultimately, it will be the responsibility of the Secretary to set the tone at the top with regard to security, and make sure that his subordinates and his direct reports certainly understand the emphasis on security and his desire to ensure that at a subsequent point, he

can come back to them and receive confirmation that security has been treated as a priority.

Mr. NUGENT. I thank all three of you for your testimony, and I think your direction in regards to what the issues are, or more importantly—I mean, you have identified the people that actually have to make it happen obviously aren't here at this point. So thank you very much.

Mr. ROGERS. Thank the gentleman. You know, it is astounding to me, we are not talking about an equipment site, we are talking about nuclear materials. And I keep hearing this issue about, well, it is a culture and we need to have more responsibility up the chain of command, nobody is talking about firing anybody. You know, as the general said earlier, when the Secretary ran off the Secretary of the Air Force and the chief of staff, it got everybody's attention. It seems like nobody is talking about we have to go to those levels of responsibility and run somebody off to make sure everybody understands that security is integral, and has got to be a part of the system. But, I don't hear anybody calling for that, but that is just me. Mr. Wilson is recognized for five minutes.

Mr. WILSON. Thank you, Mr. Chairman. And thank you all for being here today, and Mr. Friedman, I am an alumnus of Department of Energy, so I appreciate your service there as IG, a very important position. In fact, it is so important, and General Finan, for both of you, you refer to an eyes-on/hands-off approach to oversight. Can you explain why you flagged this as a concern? Why did this contribute to the security failure? And where did this approach come from? And what has been done and it has been referenced, but what has been done to fix this, beginning with the general?

General FINAN. Yes, sir. Eyes-on/hands-off was interpreted in the security community at NNSA to mean that Federal personnel were not really to interact with the contractor in executing security duties, they were only to watch them execute duties. And in many cases, not even allowed to interact with the contractor as they accomplished those duties. What that evolved to was basically a completely Federal hands-off policy; that said, in my Federal role, I can't tell the contractor what to do. I can give general directions that say, okay you need to secure a site, but the Federal personnel then failed to give additional directions that said anything about how. Well, nuclear security is absolutely critical, and it is inherently a Federal responsibility, and that means the Federal personnel have a responsibility and a duty to be a little bit more specific, and in fact, tell contractors exactly how to do nuclear security.

Now there are some variations and things like that, but what evolved over time was rather than evaluate—if you ask me to evaluate nuclear security, I am going to come up with scenarios that I think are significant and then I am going ask the contractor to execute them so I can see the contractor execute those duties. We took—eyes-on/hands-off took the Federal Government out of that role. What it did was it let the contractor decide what scenarios would be evaluated and it was all about contractor self-assessment and Federal oversight was, in fact, diminished. And so what happened is we really didn't have any insight. Federal personnel in NNSA did not have insight into the details of how the

contractor was executing that mission. And so, that really is eyes-on/hands-off and where it evolved to.

Mr. WILSON. I appreciate your raising that because I am very grateful the Savannah River Site is in the district that I represent, in Aiken and Barnwell County. And, I have had the opportunity to visit so many times, and to see the extraordinary personnel of perimeter security, so I have seen a positive. So it is startling to me that something like this could occur. Mr. Friedman.

Mr. FRIEDMAN. I associate myself with General Finan's remarks. I think she has characterized it perfectly, but if I can take a minute and describe a specific that was in our original findings. There were very, very expensive, costly cameras and detection equipment at Y–12 that was inoperable for up to 6 months and just the backlog of repairs had never been addressed. Now, the local Federal officials were aware of it, but they did not feel they were empowered because of eyes-on/hands-off essentially, they didn't feel they were empowered to force the contractor to reprioritize the work, the maintenance work that was being done to be sure the detection equipment was operating as intended. It was a vital essence, essential part of the perimeter defense mechanism at the site. And that is an example of how we have gotten to the point where, as I said earlier, we need to empower these individuals to ensure if they have a problem like that, number one, they can bring it up with the contractor and ensure that the issue is addressed. And number two, if it is not addressed, that it goes to the Administrator and that there is appropriate action taken.

Mr. WILSON. And that is particularly startling because when we think of the new technologies, we think of this as better. And so I know that your report indicates that there should be periodic in-depth reviews of contractor security, and certainly that would include that the equipment is working.

Mr. FRIEDMAN. Absolutely. It is vital. There is no excuse as far as I am concerned, in an environment such as Y–12, one of the most sensitive sites in this Nation, to have equipment inoperable and not treat it as a critical priority to get it back on line as quickly as possible.

Mr. WILSON. And for the protection of the American people, again, the new technologies we have should be used to their highest and best use, and I appreciate your efforts, all of you to do this. I yield the balance of my time.

Mr. ROGERS. I thank the gentleman and the chair now recognizes Mr. Lamborn for 5 minutes.

Mr. LAMBORN. Thank you, Mr. Chairman. I want to thank all of you for what you have done to serve and help our country. You can all jump in on this question, but General Alston, I want to ask you a two-part question. When there was the unauthorized transfer of nuclear weapons from Minot to Barksdale, the Air Force really drilled down and saw this as a broad issue that had to be addressed, even going so far as to reemphasizing the importance of the nuclear mission in the Air Force all the way back to the Air Force Academy, which is in my district. So could you address how that was done? And then how does that contrast with what is being done, if there is a contrast with the Y–12 incident?

General ALSTON. Well, sir, thank you for that question. What we recognized was that the Air Force, having been flying combat missions for such an extended period of time, and with the emerging emphasis on irregular warfare, that conventional operations and irregular warfare were elevated in their priority in terms of the way the Air Force resourced itself and the tempo and deployments. And the price you paid for that was a de-emphasis in the nuclear part of our mission set. And, we were born in that strategic attack mind-set and capability, but we had lost that focus because of other competing priorities. So when we looked at the professional military education for our NCOs and our officers, we reassessed that there was insufficient, and, in some cases, very little to non-existent elements of nuclear in those programs so that a broad brush was painted across all of our airmen as opposed to just those who have nuclear mission responsibilities today, because we felt it was important that everyone in the Air Force should have a broad sense of what we are about as airmen.

And so, we attacked that and there was a lot of re-attack as we looked and evaluated, looked and evaluated, and changed those programs so that we were satisfied the modules on nuclear were worthy at that level of education. But we didn't want to sort of cashier or contract out, if you will, strategic deterrence to just the nuclear operators; everyone needed to understand the larger context as best we could do.

Now the whole service was energized in the face of this epic failure, and we considered it an enterprise failure. This was mission failure at historic levels for us and we looked at it that way.

The challenge, I think, with the Y–12 situation is we didn't necessarily find a pervasive evaluation that this was mission failure that could be a wakeup call across the enterprise. The guys at Oak Ridge made a very bad mistake, but the guys at Pantex or the guys at Savannah River have not made that transgression. So weaknesses that might be systemic in other places with the distance that the sites preferred we didn't witness a strong embrace to say, truly, how can we ventilate the deficiencies there and see them here. I believe that work took place. I just think that the self-critical capacity can be improved in the NNSA and the Department of Energy to make that assessment broad and legitimate.

Mr. LAMBORN. For either of you other two, General or Inspector General?

General FINAN. I agree with what General Alston stated. And when I took a look, I took a look just at the Federal organization and the Federal assessment model contained within NNSA, and there were structural flaws in both the organization and the assessment model, which is why I recommended a complete change in the organizational model and a new assessment model to reach out beyond Y–12 to all the other organizations because it does, in effect, affect all eight NNSA sites.

Mr. FRIEDMAN. Again, I agree with my colleagues at the table, I would say that one of our, I think more important recommendations which actually sounds very subtle and may sound actually unimportant is that the lessons learned from Y–12, and it was a tremendous wakeup call because Mr. Cooper described the three intruders, they could have been three people who were armed in a

different way and had malicious intent, and could have been a real tragedy, so we had a tremendous wakeup call. Our point—one of the points we made was that it is important that the lessons learned from Y–12 be exported throughout the entire Department of Energy complex, so that we are in a mode of preventing this sort of thing from happening again, not just simply reacting, should it occur in another location.

Mr. LAMBORN. Thank you, thank you, Mr. Chairman.

Mr. ROGERS. The chair now recognizes Mr. Veasey for 5 minutes.

You know, the point you just made goes back to what I said earlier, and that is, we have learned some real lessons at Y–12, but apparently, we have been hearing this call for these changes for a long time. The thing I want to assure the folks who are listening to this is this committee is not going to let this go, the DOE and NNSA are going to fix this problem going forward in a meaningful way. And until they do, we are going to make them wish they had. So this is not going away. We are—does the ranking member have any more comments?

We are about to be called for votes, I want to thank our witnesses for their time and their energy and attention, and we appreciate you and we will go into recess now for our votes and bring our second panel back up after votes. Thank you.

[Recess.]

Mr. ROGERS. I would like to call this hearing of the Armed Services Subcommittee on Strategic Forces back to order. And apologize for the delay, but our votes are over for the day. And I thank our panelists for hanging around and look forward to their comments.

I do want to thank you for your time and energy in preparing for this hearing. I know it takes a lot of time and effort, but you know it is important to us that you have done it. So thank you for that.

What I would like to do, your full statements have been submitted for the record. Jim and I both read them, the ranking member and I have both read them, but I would like to ask each one of you to take about a minute and synopsize the content of your opening statement, and then we will just go directly to questions, for time sake.

Oh, I am sorry. Didn't introduce the witnesses. I thought I had done that earlier. We first have Secretary Daniel Poneman and Honorable Neile Miller. She is the Acting Administrator, and Principal Deputy Administrator for the NNSA.

Secretary Poneman.

## STATEMENT OF HON. DANIEL B. PONEMAN, DEPUTY SECRETARY OF ENERGY, U.S. DEPARTMENT OF ENERGY; AND HON. NEILE L. MILLER, ACTING ADMINISTRATOR AND PRINCIPAL DEPUTY ADMINISTRATOR, NATIONAL NUCLEAR SECURITY ADMINISTRATION

### STATEMENT OF HON. DANIEL B. PONEMAN

Secretary PONEMAN. Thank you, Mr. Chairman, Ranking Member Cooper, and members of the subcommittee. We are grateful for the invitation to appear before you today to provide the subcommittee details on the actions the Department has taken or will

take to strengthen the security of the nuclear weapons complex in the wake of the July 2012 Y–12 incident. We appreciate the interest and engagement of this committee and recognize the important oversight role that you fulfill.

The Secretary and I recognize the severity of the problem that led to this point and we have acted swiftly to identify and address the issues it revealed. Since the Y–12 incident, several major actions have taken place to improve security immediately and for the long term, and I will just mention, in deference to your request, Mr. Chairman, just a few.

We restructured the contracts at Y–12 to integrate security into the line of command of the M&O [management and operations] contractor. The protective force contractor was terminated and a new M&O contractor has been selected to manage the Y–12 site, providing an opportunity for new leadership and to improve Y–12 security culture. We held accountable both the senior Federal and contractor management personnel at headquarters and at the site, removing them from their positions. The Department's Chief of Health, Safety, and Security [HSS] conducted an independent security inspection of the Y–12 security operations, including rigorous force-on-force performance testing, as well as no-notice and short-notice limited scope performance testing activities as directed by the Secretary, and they will be conducting a follow-up review in April.

The Secretary also directed HSS to conduct immediate extent of condition assessments of all Category 1 sites across the DOE complex to identify any immediate security issues and to follow up with full security inspections, including force-on-force exercises, to assure effective security measures are being implemented at those sites. NNSA conducted an immediate after-action report to identify causes, followed by the report, which I know you have heard about this morning, from General Finan. The former Deputy Administrator tasked General Finan with reviewing the Federal NNSA security organizational structure and security oversight model. And you have heard about her recommendations, which we are implementing, so we can talk further about that during your questions.

Finally, we had an independent group—actually they were individuals, all of whom have distinguished, long careers in national security and in nuclear matters. Each one provided thoughtful advice on the DOE's nuclear security structure, specifically all Category 1 nuclear facilities, and we are now reviewing and discussing their advice on how to improve security at Y–12 and across the nuclear enterprise.

So in conclusion, the series of personnel and management changes that I have described today have been made to provide effective security at the Y–12 site and across the DOE complex. We are working to carry out the structural and cultural changes required to secure all Category 1 nuclear materials at this and all of our facilities. Our management principles hold that our mission is vital and urgent. Nowhere is that more true than here.

The security of our Nation's nuclear material and technology is a core responsibility of the Department in support of the President and in defense of the Nation. The incident at Y–12 was unacceptable and served as an important wakeup call for our entire com-

plex. The Department is taking aggressive actions to ensure the reliability of our nuclear security programs across the entire DOE enterprise, and will continue to do so.

In that effort, the Department looks forward to working with this subcommittee, sir, to ensure the security of the Nation's nuclear materials. And, Acting Administrator Miller and I would be very pleased to answer any questions from you and members of the committee.

[The prepared statement of Secretary Poneman can be found in the Appendix on page 101.]

Mr. ROGERS. Thank you.

Ms. Miller, did you have an opening statement?

Ms. MILLER. No, sir. Mr. Poneman is giving the statement.

Mr. ROGERS. Great. Well, thank you. And, I will start off with the questionings for Secretary Poneman.

As Deputy Secretary for the Department of Energy, you talked about this being unacceptable, and you just made some reference to some corrective actions, and you talked about how you have now completed an integration in the line of chain of command with a new contractor. What is different in this line of chain of command?

Secretary PONEMAN. Okay. At the time of the incident, Mr. Chairman, there were two separate contracts at the site. One was the overall management operations contract for the site.

Mr. ROGERS. Okay. You are talking about the line of chain among the contractors, not within the Department. Have you altered that in any way? That once the contractor notifies the Department of anything, good or bad, has the chain from that contact person up the stream been modified at all?

Secretary PONEMAN. Yes. But the way the contract is structured affects it. But I will go right to the part you asked. One of the things that General Finan found in her report was that there was lack of clarity, that the organization known as NA–70 for nuclear security was exercising some authority in line management over security activities at the site, as was activities under our infrastructure and operations, the so-called double zero. That was confusing. We have ended that. We have made it very clear that the line management must go down from the Administrator through the Infrastructure and Operations Office. And that has removed the security organization, NA–70, from that.

NA–70's role has been clarified so that their role is to develop the plans, it is a staffing function, and then to evaluate the performance. That had the additional change in the field, Mr. Chairman, that the evaluation of performance under the contract was no longer done by the field Feds, which was creating, in General Finan's review, too close of a situation between the people on the site, between the contractor and the Fed.

And so I think we have really clarified it, but the other fact that actually bears on this as well is there was also confusion that was created by having these two separate contracts at the site, and we have immediately folded the Proforce [protective force] security boots-on-the-ground contract under the M&O contract, just to clarify.

Mr. ROGERS. Okay. Under this new structure, if we were to have another incident, who would be the ultimate person responsible for security at that Y–12 site?

Secretary PONEMAN. The line management is always responsible, going straight down from the Secretary down through the NNSA Administrator.

Mr. ROGERS. Walk me through it. Secretary——

Secretary PONEMAN. Deputy Secretary, NNSA Administrator, the director of the Federal site for the NNSA, and then it goes straight from that person to the senior contract official.

Mr. ROGERS. And that was not the case when this incident occurred?

Secretary PONEMAN. There was confusion because there were directives that were coming out of the NA–70 organization that could have been confusing in terms of where the accountability was from the perspective of the people at the site.

Mr. ROGERS. Aside from the contract with the contractor being terminated, which it was about to expire anyway, you mentioned that responsible people were reassigned. You put removed from their responsibilities, but they weren't fired. Why weren't they fired?

Secretary PONEMAN. Sir, the first thing we had to do in the incident was we, as you have said many times, hold the people accountable. So we did that both at the site and at the headquarters. The top three officials at the headquarters responsible for nuclear security were removed from those positions. The top two relevant officials on the Federal side at the site were removed from their positions.

Mr. ROGERS. Why weren't they fired, though? Why were they just removed? This is a nuclear facility.

Secretary PONEMAN. That is true, sir. There are additional disciplinary actions that have been underway. We have due process and various procedural safeguards that occur in our system, and those are now being pursued. But the important thing in terms of protecting the nuclear material was to get those people out of that line. Most of them are out of the NNSA entirely. And in addition, we ensured that people at the contractor level knew they had lost our confidence. And the top two officials responsible at Y–12 on the contractor side were also removed.

Mr. ROGERS. Well, you know, you heard me earlier talk about Secretary Gates. He fired the Secretary of the Air Force and the Chief of Staff of the Air Force when he had a similar incident. I think that is the model. Do you disagree that should be the model in how we respond to serious security violations at important facilities like this?

Secretary PONEMAN. I certainly agree, Mr. Chairman, that accountability is absolutely crucial. I am not deeply intimate with the details of the 2007 Air Force incident. I have the highest regard for Secretary Gates. But I think the principles that he described in terms of accountability are very much ones that we share.

Mr. ROGERS. Well, I would hope so, and I would hope you start reflecting those going forward, because that is the kind of action that sends a clear message that these lapses in security will not be tolerated, because the other factor here is this has been going

on for 10 years. We have had study after study after study. So, frankly, the folks at the top of the food chain really should have known about this before it happened and shouldn't have been allowing it to happen.

But with that, I will turn to my ranking member, Mr. Cooper, for any questions he may have.

Mr. COOPER. Thank you, Mr. Chairman. I welcome the witnesses. I am sorry we have to be here, because this incident never should have happened.

You say that you are for accountability, but wasn't the main contractor there, Babcock & Wilcox, still able to receive 60 percent of its award fee, or $36 million, right after the incident happened?

Secretary PONEMAN. Mr. Chairman, the way that——

Mr. COOPER. I am not the chairman. I am the ranking member.

Secretary PONEMAN. Oh. Sorry. Mr. Ranking Member. The award fee under the terms of the contract—and I think it is a very fair question to pursue how we structure these in terms of compensation, I think that is an absolutely fair point—the only amount of fee that was available for security was zeroed out. So that was removed from the contract.

The way they got to the 40 percent reduction of fee was by taking all of that and then going beyond that. There are other things happening at the site in terms of naval reactor fuel, in terms of directed stockpile work, and so forth. And the way that the contract is structured, the fee is bucketed. And we took the fee that was available to take away, away, and that was a series that we have actually followed up in subsequent incidents also seeking to claw back fee, because we agree the American people should not be paying for underperformance when it comes to security.

Mr. COOPER. And how much of the fee do you expect to claw back?

Secretary PONEMAN. Well, the numbers that you have cited there, there is 40 percent in the episode at Y–12 for the contract.

Mr. COOPER. But I thought you said there were further efforts going on.

Secretary PONEMAN. There was a $10 million fee that was clawed back for another episode elsewhere in the complex.

Mr. COOPER. But immediately prior to the incident, your agency in its wisdom had given Babcock & Wilcox an excellent rating for its safeguards and security work, and they received their full $51 million incentive fee in fiscal year 2011, even though, as has been testified to, the cameras weren't working on a wholesale basis, took months and months to ever do repairs. Why do they get their entire incentive fee right prior to the incident?

Secretary PONEMAN. Congressman, this flags exactly one of the deficiencies in the structure that preceded this incident, because there was, as again General Finan's report I think makes very clear, a tendency to not have the boots-on-the-ground analysis and review, but to have the evaluation based on what the contractor said, and then have an on-paper review. That is why separating that role out from the site and putting it into the nuclear security organization at headquarters would hopefully correct that.

We did not see the things in advance the way we should have. Obviously, had we seen those things in advance, we would have re-

placed all 62 cameras ahead of time. I am hoping, and I believe that both the organizational and the cultural changes that we are going to institute pursuant to the Finan report will prevent this kind of thing from happening in the future.

Mr. COOPER. With all due respect, it doesn't sound to me like you are taking responsibility, because aren't you the Deputy Secretary and haven't you been the Deputy Secretary for some time?

Secretary PONEMAN. Yes, sir. And from the moment I heard about this incident, I have been doing everything I can in every dimension to make sure that nothing like this ever happens again. I do feel deeply responsible.

Mr. COOPER. You have been doing everything you can, and the questions to my colleague, Ms. Sanchez, were submitted 5 months after the hearing testimony? The copy we got, you needlessly duplicated one question twice. Doesn't look like much effort was put into this. And I know this is just an exchange of paper, but——

Secretary PONEMAN. Congressman——

Mr. COOPER. Do you feel like you are taking responsibility?

Secretary PONEMAN. Yes, sir, I do. I take responsibility for everything that happens in the Department and I am——

Mr. COOPER. Has your pay been reduced? Are you threatened in any way? What sanctions have you faced?

Secretary PONEMAN. Congressman, I am doing everything I can to address the problem, and I will do that as long as I am in this position. And I will be very open to working with this committee and all others to make sure that nothing like this can ever happen again.

Mr. COOPER. But meanwhile, as the inspector general told us in his testimony, your Department is spending about a billion dollars a year securing various facilities, hiring 4,000 guard personnel through various devices, and in some places it is one prime contract, in some cases it is split two primes, and in some places it is a subcontract. There seems to be no rhyme or reason to this. But if you divide, you know, the salary component of that, $700 million by the 4,000 employees, that's $175,000 per guard. Where is this money going and what results are we getting for this? That is a lot of money, and my guess is the guards aren't actually being paid nearly that much. Who is making the difference?

Secretary PONEMAN. Congressman, there are a number—I don't have the exact calculation you have before you—there are a number of both physical assets in terms of huge facilities with thick walls, BearCats and various perimeter fences and various security systems, all of which requires an investment.

But to be clear, the money itself is not going to solve the problem if we don't have the clarity in the lines of responsibility and in the authorities that go with it and, frankly, the cultural shift that is required to go with it. It is not a problem that will be solved by dollars. And the dollars that are invested in it are very important, because we need to get the assets, both the human assets and the physical assets, but that's only part of the problem.

Mr. COOPER. Trust me, I am not suggesting spending more money. I am asking what value the taxpayer got for this extraordinary outlay over many years. And this is, according to your own IG, money spent on employee compensation.

Secretary PONEMAN. Congressman, we have large, large quantities of both highly enriched uranium and separated plutonium, all of which is extraordinarily sensitive. That material is very, very well defended. It is of absolute paramount importance.

Mr. COOPER. It's well defended when an 82-year-old nun got into Y–12? How can you possibly say that?

Secretary PONEMAN. Congressman, the episode that occurred, as we have repeatedly testified in this and the prior hearing, is absolutely unacceptable. It is a wakeup call. There are several——

Mr. COOPER. Then how can you say it was well defended? It was not well defended. That is why we are having this hearing.

Secretary PONEMAN. Congressman, what I am trying to say is that there are a number of additional layers of security. It is unacceptable that they penetrated the perimeter fence. That is unacceptable, a wakeup call. We are taking the appropriate actions. The concertina wire is around it. There are other additional layers, including, you know, military-style forces, including various physical impediments. And I can assure you that there are many more layers that are defending that very, very sensitive material.

Mr. COOPER. So we really had nothing to worry about. There were many more layers of security left and it was all fine.

Secretary PONEMAN. Congressman, that is not at all what I am saying. You have heard us from day one, Secretary Chu and I have been consistent, this was unacceptable. And, it is a shocking breach of the security that we thought was in place.

That having been said, your specific question went to the actual material itself, and I am only saying, not that there is any reason for complacency, far from it, quite the opposite, but to say that we do have additional measures of protection that is needed for that material. It is unacceptable what happened, and we have to make sure that that part gets fixed as well.

Mr. COOPER. Mr. Chairman, in all due respect to the witness, it still does not sound like he is really taking responsibility for this.

Secretary PONEMAN. I want to be very clear, Congressman. I accept responsibility for this.

Mr. COOPER. Well, what punishment have you suffered for it?

Secretary PONEMAN. I am working——

Mr. COOPER. Other than attending this hearing?

Secretary PONEMAN. I am working on this problem, sir, as hard as I can.

Mr. COOPER. Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman. The chair now recognizes the former chairman of this subcommittee, Mr. Turner of Ohio, for 5 minutes.

Mr. TURNER. Thank you, Mr. Chairman.

Secretary Poneman, I want to thank you for your efforts to try to address this. I happen to know that you are a very hands-on Secretary, you and I having worked together on an issue with respect to the Mound facility. I was very impressed by the fact that you do rise to a very hands-on level. So that's why I think this whole problem leaves most of us scratching our head, wondering: where are we and why do we have this circumstance?

So I am going to ask you a couple questions that I think frame the topic in the level of oversight where we have concerns. So I am

going to ask you a broad, basic question. Is there ever a situation where a security failure at one of the facilities protecting our nuclear infrastructure would result in the termination of an employee of DOE or NNSA due to their performance?

Secretary PONEMAN. It could, sir. What we can do——

Mr. TURNER. I am sorry. So the answer then is yes?

Secretary PONEMAN. The——

Mr. TURNER. Because it's a pretty direct question. I am not asking you is it in the realm of possibilities. I am asking you, is there ever a situation where a security failure at one of our—the protection of one of our nuclear facilities would result in the termination of an employee of DOE or NNSA due to performance? It's a yes-or-no question.

Secretary PONEMAN. Congressman, if—it depends——

Mr. TURNER. There is no "depend." It is like a——

Secretary PONEMAN. No.

Mr. TURNER. Because it already says "ever", so "ever" encompasses the whole scope——

Secretary PONEMAN. Yes.

Mr. TURNER [continuing]. Of possibilities. Is there ever a situation?

Secretary PONEMAN. It could, yes.

Mr. TURNER. Yes. Okay.

Now, in taking that broad statement where you have acknowledged that there is a situation where a failure could result in termination due to performance, I am then going to ask you the next step of that, because I am not just asking your opinion, because you are actually—you know, you are in the chain of—line of command here of understanding the execution of this.

So would one of those situations be where all of the safeguards were down, where someone could get all the way into one of our buildings, and nobody does? What I am asking you in this, and I am going to be clear, we had a breach where people actually got all the way into this building. Right? All the way to the building.

Secretary PONEMAN. To the building, sir.

Mr. TURNER. That is what I am saying, to the building. Is there ever a situation where someone would lose their job for performance where no one penetrated, there was no breach, but the safeguards were down that would have permitted it? Because that is certainly what I would consider to the level of a failure of performance.

Secretary PONEMAN. Congressman, what I can't do is answer a hypothetical. It depends on——

Mr. TURNER. It is not hypothetical. It really is very, very clear. You have a job that has no margin of an error: protect these facilities. Right? And we only can protect these situations through the application of technology operated by people. And the people were, you know, we're subject to their performance as to whether or not it works.

So if someone isn't performing and the system is down, even if there is no breach, but it is their responsibility and their fault that the system is down and someone could get all the way——

Secretary PONEMAN. Right.

Mr. TURNER [continuing]. When I say "into," I mean touch the building, not inside the building, is that enough for someone to be terminated due to performance?

Secretary PONEMAN. Sir——

Mr. TURNER. Because I think, this committee thinks that if we have an agency that is governmental that has the responsibility for protecting these facilities and we have a system where those in charge think that you don't even have to do your job to keep your job, then we don't have something that is working. So it is a simple question. If the system goes down where someone could go in and touch the side of the building and no one does, it is not a real breach but the system has come down due to their performance, is that the type of lack of performance that should result in termination?

Secretary PONEMAN. I can tell you that can and has resulted in removal from position.

Mr. TURNER. So the answer is yes?

Secretary PONEMAN. I said removal from position. That is what we did.

Mr. TURNER. Well, that is not termination.

Secretary PONEMAN. And that gets into a level of law and due process——

Mr. TURNER. So you are testifying before this committee today that if the entire security system of our nuclear infrastructure facilities went down on the perimeter of a building that allowed someone to go in and it was a result of their performance, it is not a terminable offense——

Secretary PONEMAN. I did not say that——

Mr. TURNER [continuing]. Under your agency?

Secretary PONEMAN. I did not say that, sir. I said we can remove them——

Mr. TURNER. Then please tell me the opposite——

Secretary PONEMAN. I am telling you——

Mr. TURNER [continuing]. Because that has to be true. It has to be that it would result in someone losing their job. If not, we need to pass a law here. We need to, like, stop doing oversight and actually do legislation, because if you don't have performance to be able to protect the facility, then we don't really have protection, we don't have security. Is it a terminable offense—terminate-able offense?

Secretary PONEMAN. You and I are both lawyers. You are asking a technical legal question. I want to make sure I am absolutely accurate——

Mr. TURNER. If you don't have clarity on this, then I think that this committee needs to put something in our next piece of legislation that absolutely makes it clear that if, due to the performance of individuals, that the security system fails, that it would be an offense resulting in termination, because that clarity, I think, certainly is with the American public.

Secretary PONEMAN. Congressman, as I told Chairman Rogers and as I told you when you were chairman of this committee, we are always ready to work with you and with this committee to make sure we have the right kind of laws in place. I am not trying to be evasive. We moved the people out of the positions. There are due process protections. And if we can come back to it in more de-

tail, there may be a very simple yes/no answer, but I am not acting as a lawyer today, and I don't want to give you an inaccurate——

Mr. TURNER. I wasn't asking you a lawyer question, I was asking you a scope of responsibility and authority question. I mean——

Secretary PONEMAN. And in that, I am very confident——

Mr. TURNER. It shouldn't require lawyers to understand whether or not, if there is a failure of performance to that level, that that would be an offense for which there would be termination.

Mr. Chairman, I yield back.

Mr. ROGERS. I thank the gentleman.

I am going to clarify with the Secretary. Is the due process you are talking about, is that the union contract?

Secretary PONEMAN. No. I am talking about the procedural due process that any Federal employee is entitled to when he is facing some——

Mr. ROGERS. Well, they can have that due process in response to their termination, can't they? I mean, you terminate them, and then they have got the due process to appeal it——

Secretary PONEMAN. We have to——

Mr. ROGERS [continuing]. And try to fight that termination. But it just seems to me like you are claiming that they have got a right to go through all this before you can terminate them.

Secretary PONEMAN. Well, what we can do and what we did do, Mr. Chairman, was remove these people from the responsibility for anything having to do with security immediately, pending finding out what further disciplinary action was available, and that disciplinary action is subject to due process.

Mr. ROGERS. Well, I am a recovering attorney, too. I think that due process would not impede firing people who would let an 82-year-old woman get into a nuclear facility.

But having said that, the chairman recognizes the gentleman from South Carolina, Mr. Wilson.

Mr. WILSON. Thank you, Mr. Chairman. And I share the chagrin of the former chairman and the current chairman. It seems to me that with the breaches that occurred, that there should have been terminations. Just shifting persons around doesn't really achieve the level of accountability of something as extraordinarily important. And I have the perception of having actually worked at the Savannah River Site, and so by working there, I actually had a good feeling about the perimeter security, the persons who were monitoring and indeed acting, and I felt secure. And I know that the people who worked there, lived there, raised their families there, retire there feel secure.

But I am concerned that I have also seen studies that there is a culture with DOE, with NNSA that has not stressed security. And so how can we reassure people who live in these communities that indeed a culture of lack of appreciation of security is being addressed?

Secretary PONEMAN. It is a great question, Congressman. You can reassure them by saying that the top three security officials at the headquarters responsible for Y–12 at that time were removed from their positions, that the two top Federal officials at the site were removed from their positions, that the contractor that actually had the boots-on-the ground professional force was terminated full

out, that the top two officials at the management and operations facility, they were also retired and taken out of the picture. Everybody in that chain of command, from the individual responders and to the senior officials responsible for security specifically at that site, were removed.

At the same time, that would not be enough. We have undertaken the organizational and structural changes, we have replaced all the cameras, we have put concertina wire around the whole facility, all the Perimeter Intrusion Detection and Assessment System (PIDAS) improvements, the central alarm station has been upgraded. All of the things we should have known about but found out about through this unfortunate and terrible incident, we have taken those steps. So I do think that the American people can take assurance from that.

Mr. WILSON. Administrator Miller.

Ms. MILLER. I just support what the Deputy Secretary has said. First and foremost, culture is going to be affected by the leadership and management and their attitudes toward security, safety, and everything else that we do. And we are looking very hard and have been making serious changes within the NNSA to directly address leadership and management issues as they affect security, safety, and everything else we do.

Mr. WILSON. And I am equally concerned that there seems to be a lot of reliance on self-assessment by contractors, that the overseers are depending on the contractors. Is that being changed?

Secretary PONEMAN. That is being addressed, sir. And I think that did contribute to the problems that we faced before. General Finan's recommendation is, we believe, a sound one, which is to start with the basis of the contractor's assessment, but then instead of having that assessed in the field where there is a possibility of the Feds being too close to the contractors, that function is being clearly vested in the headquarters organization, the NA–70 organization, and then that is going to be further subject to further overview by the Health, Safety, and Security Office.

Mr. WILSON. And, Ms. Miller.

Ms. MILLER. Yeah. I would like to also emphasize, we have the sites now reporting directly to the Administrator, and in this way, we expect security, as well as other things, but security to be a clear line of accountability from the Administrator through to the site manager, the sites, as the implementers of the policy that the security policy organization, that the Deputy Secretary was just referring to, those policies and orders that they issue are then—which is their responsibility, and it is also their responsibility to assess the performance of the sites in implementing those orders—is just as clear that the line of accountability for implementing it at the site goes directly from the site to the Administrator.

Mr. WILSON. And related to that is, there was the recommendation that headquarters staff visit sites and rotate between the sites. And is that being done?

Ms. MILLER. Headquarters staff is now both in the implementing side, as well as in the policy and assessment side, regularly scheduled and going to sites. And as well as the rotations are, we have put this in throughout the NNSA. We are very conscious of the fact

that people staying in one place for too long may lead to people becoming complacent.

Mr. WILSON. And thank you both. And I do know that when the headquarters staff visits, it creates an extraordinary level of attention. Thank you.

Mr. ROGERS. Thank the gentleman.

The chair now recognizes my friend and colleague from Arizona, Mr. Franks, for 5 minutes.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Secretary Poneman, I want to try to get three questions in here, if I can quickly. First, I have had the opportunity to see hearings on this before, some in a private setting, and so I have probably already expressed the commensurate level of bewilderment. And, you know, I don't seek to patronize anyone to remind us all that the materials that are kept in these facilities are, you know, are highly technically challenging to create, and yet to weaponize them is a much lesser difficulty technologically to do. So, I mean, the implications here are pretty profound, and I think everyone knows that.

I guess quickly one question I wanted to ask. It seems like the contractors that had reported these lapses in safety precautions were treated very differently than those they reported to, who in some cases ignored their warnings. Is that your perspective?

Secretary PONEMAN. I am not sure, Congressman, I am tracking which contractors you are referring——

Mr. FRANKS. Well, the contractors, on-the-ground contractors that were there that were watching the cameras. I am told that there was a significant reporting on their behalf prior to these incidents, saying, you know, that we had some technical challenges and that we really weren't up to——

Secretary PONEMAN. Yes, sir. Some of those deficiencies had been earlier noted in earlier reports. That is true.

Mr. FRANKS. And yet they were, you know, handled pretty roughly, it sounds like, and the folks that they reported to weren't. And I will leave that there, sir, because I want to get to another.

The previous panel emphasized sort of the line of responsibility. And I think that that is something that is almost ubiquitous throughout the entire human dynamic. You know, somebody has got to have responsibility. Everybody's responsibility is nobody's responsibility. But it appears to me that DOE and the NNSA have not really addressed that effectively within NNSA, because DOE continues to have an oversight office under HSS, and NNSA now has a split security between an office responsible for policy and oversight and another office that is responsible for program execution.

And I am just wondering, how do all these DOE offices ensure that there is accountability for making sure that the security program is properly executed at these DOE sites?

Secretary PONEMAN. Okay. So I now understand the first part, and I will just say very quickly, both contractors involved had their leadership removed. So they both paid the appropriate accountability price, just on that first part of your question. And I know you wanted to get to the second one.

On the second one, it is a very good question, and as you just heard the Acting Administrator say, we believed that part of the problem here, as General Finan pointed out, was that there was this confusion. The clarity of the line management down through this infrastructure and operations, that's the line management. They are responsible for execution. They had to take away the interference with that line management was coming out of the NA–70 nuclear security organization. So they just make the plans and evaluate it, but that is all inside NNSA. And so to have a further check, because these materials are so sensitive and do need to be secure, is to have a check on the check by having HSS perform an outside independent oversight role outside of the National Nuclear Security Administration.

Mr. FRANKS. But just a yes or no quickly. Is it your testimony before this committee that the line of responsibility, that any ambiguities there have been dealt with?

Secretary PONEMAN. We are in the process of implementing General Finan's recommendations. I would like to come back to this committee when I can tell you that we feel like——

Mr. FRANKS. To me, Mr. Chairman, that seems seminal to this whole discussion.

Secretary PONEMAN. We agree.

Mr. FRANKS. Let me shift gears quickly, and I will ask both of you, because I will run out of time here and you both can answer the question still. When you think about these potential breaches of security in the future, you know, there are all kinds of issues out there, and I am just wondering one specific question, and I would welcome you to mention any others that are on your mind. But, you know, there is a significant increase in technology across the world with intentional electromagnetic interference, or these EMP [electromagnetic pulse] device capability, which seems to me that it could really put these facilities at risk, and even further, you know, the potential of a major EMP event, either geomagnetic disturbance or a high-altitude nuclear burst.

Can you tell me, are we protecting our critical defense apparatus like the Y–12 facility against these three prongs of EMP: the E1, E2, and E3?

Secretary PONEMAN. Congressman Franks, I am well aware of your thought leadership on this challenge. I have talked to former Secretary Jim Schlesinger and Mr. Ikle, may he rest in peace, and what I am here to tell you is that we are very focused on addressing all of those kinds of threats, which don't, as you well know, affect only Y–12, but frankly everything, far, far beyond that. We would love to work more closely with you on this subject. The executive orders and the Presidential Directive 21 that the President just issued addressed exactly this kind of problem. It is something that is a huge problem. It is going to take a lot of work to get into a safe place, but we are very focused on it, sir.

Mr. FRANKS. All right. Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

Before I go to Mr. Garamendi, I want to clarify. You stated a minute ago that you are in the process of implementing General Finan's findings. That is just at NNSA, that is not at DOE. What

are you doing at DOE to deal with the problem that Mr. Franks just addressed?

Secretary PONEMAN. The problem that Mr. Franks just addressed actually goes well beyond NNSA and will require various parts of our organization, including our Chief Information Officer, which has technical capacity to deal with the EMP issues.

Mr. ROGERS. No, no. I am talking about his earlier issue dealing with the chain of command on reports by the contractor——

Secretary PONEMAN. Okay.

Mr. ROGERS [continuing]. Of deficiencies that are not being remedied.

Secretary PONEMAN. Mr. Chairman, those issues are among those that have been addressed by what we call the three wise men, of whom you had one here testifying this morning. We are having internal discussions precisely on this question of how to make sure that the larger DOE organization works effectively in ensuring the same kind of oversight that we are talking about inside of NNSA, because as you know, Mr. Chairman, there is some Category 1 material that is outside of the NNSA and we have to make sure it is all well protected.

One thing that has been done is there was some confusion as between overall directives that are departmental-wide and those directives that are specific to NNSA. General Finan's recommendation, which we are following, says we need to be clear that the DOE directives are those that are binding is the baseline. Anything beyond that, because of the special needs and requirements of NNSA, should be done as only a way to augment or strengthen and should not be any way to confuse or distract from the overall directive that governs the whole Department.

Mr. ROGERS. The gentleman, Mr. Garamendi, is recognized for 5 minutes.

Mr. GARAMENDI. Thank you, Mr. Chairman.

I appreciate the testimony both of you have given, and I was reading your testimony also. While you have explained verbally and in some writing the organizational structure, it is not clear to me exactly how that chain of command and organizational structure is actually in place; therefore, I would appreciate it if you could deliver to our committee staff a detailed organizational chart——

Secretary PONEMAN. Absolutely.

Mr. GARAMENDI [continuing]. With the accompanying job descriptions.

Secretary PONEMAN. Happy do it, sir.

Mr. GARAMENDI. I think that would be helpful, at least for me, to understand the words that you have said and how it works out. From the previous questions asked, it is not just within the NNSA, it is also within the Department and the organizational structure therein. So if you would do that, I would appreciate it.

Secretary PONEMAN. We would be very happy to provide this.

[The information referred to can be found in the Appendix on page 117.]

Mr. GARAMENDI. That would at least allow me the opportunity to understand more completely your testimony. And I thank you.

I yield back, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

I want to follow up. We heard in the earlier panel of all the studies over the years. Why do you think it is that these longstanding, well-documented deficiencies in security at this particular facility were allowed to go on so long?

Secretary PONEMAN. Well, the things that we have found since the episode, Mr. Chairman, were that, even though some of these things were noticed, that our internal reporting chain was broken, was the phrase that I think was used in some of the reviews. And so you can rest assured that if we had known what was actually the situation on the ground——

Mr. ROGERS. So you weren't aware of any of those studies from 2002, 2005——

Secretary PONEMAN. Well, I thought you were asking specifically about the——

Mr. ROGERS. No. I am talking about the 10 years, the 4 studies over 10 years, with General Finan's been the most recent. The three prior to that, were you aware of those studies and their findings?

Secretary PONEMAN. After the——

Mr. ROGERS. Admiral Mies, yeah.

Secretary PONEMAN. After the Y–12 episode, I became aware. I actually——

Mr. ROGERS. So before that, you weren't aware of them?

Secretary PONEMAN. Well, the one study I was aware of, and I don't know if this is one of the ones that you are referring to, I helped former Senator Baker and Mr. Hamilton look at the episode of the lost hard drive at Los Alamos, and I was aware of that one. And the thing that we found there was, in fact, the same kind of problem of division of the security mission from the line organization was a source of challenge. What I did not realize was that that particular problem was still persisting to the degree that it obviously was.

Mr. ROGERS. Why? Why were you not aware?

Secretary PONEMAN. I was not aware that the cultural and sort of the situation at Y–12, which we found out post hoc, was occurring at the time, because it had not come to my attention. I can assure you if it had, I would have acted.

Mr. ROGERS. Who do you think should have reported that to you? These were general officers who were doing these studies, very high ranking, important, thoughtful people who were making these reports. Were they just to be put on the shelf or were they to be given to policymakers who could implement changes?

Secretary PONEMAN. I would have to know, sir, which studies you are referring to and if they were done during——

Mr. ROGERS. Admiral Mies in 2005, for example.

Secretary PONEMAN. Yeah. Sir——

Mr. ROGERS. Who should have told you about that?

Secretary PONEMAN. I don't know who would have told me about a 2005 report.

Mr. ROGERS. Should Ms. Miller have told you about it?

Secretary PONEMAN. Sir, it was a 2005 report, and I just don't know what happens in terms of the shelf life of these reports and when they get repeatedly briefed. We are responding to the respon-

sibilities we have got. Anything that we have done to look at the problem, we obviously have to be fully accountable for. It is always, always a good thing to go back and see what has been done through time. That is why when this episode happened, we did look at those reports and we found a number of things that need to be addressed.

Mr. ROGERS. Let me ask this. Ms. Miller, who do you report to on security matters? Who is your immediate superior?

Ms. MILLER. My immediate superior is the Deputy Secretary.

Mr. ROGERS. Okay. Were you aware of Admiral Mies' study?

Ms. MILLER. I became aware of Admiral Mies' study. I joined the NNSA in 2010.

Mr. ROGERS. 2010.

Ms. MILLER. Uh-huh.

Mr. ROGERS. And when you arrived in 2010, how long was it before you became aware of Admiral Mies' study?

Ms. MILLER. I knew of Admiral Mies' study a little bit before then. I did not become aware of the contents of it for probably the first year that I was there.

Mr. ROGERS. And so you knew about it by 2011, midyear.

Ms. MILLER. Uh-huh.

Mr. ROGERS. Did you take any action to inform Secretary Poneman that you have a cultural problem that has got to be addressed?

Ms. MILLER. I did not take any actions to inform Secretary Poneman. I did begin to take actions within the NNSA to address cultural problems that, again, affect——

Mr. ROGERS. What actions specifically? Did you fire anybody?

Ms. MILLER. No. No.

Mr. ROGERS. Let me ask this.

Ms. MILLER. There were no firing offenses.

Mr. ROGERS. The chief of security for DOE has been there for 20 years. Clearly, given these studies that I have referred to—and what were they? The Commission on Science and Security did one in 2002, Admiral Mies in 2005. And, yeah, there was a couple others we went through in our earlier panel. But my point is, so your chief of security clearly should have been handed a copy of those studies, wouldn't you think, Secretary Poneman?

Secretary PONEMAN. Presumably when they came out, that would have happened.

Mr. ROGERS. That would have been on his watch to know we have got an installation under my domain of responsibility and we now have a study that says there is problems. Would that make sense, that he would get a copy of it?

Secretary PONEMAN. I would presume that all of those studies you referred to were reported to the Department contemporaneously.

Mr. ROGERS. Yeah. Would you turn your microphone on, please?

Secretary PONEMAN. Sorry. I would assume, sir, that those reports when they came out would have been reported to the Department contemporaneously.

Mr. ROGERS. Right. And the person, the relevant person would have been the chief of security, wouldn't it be?

Secretary PONEMAN. It certainly would have been relevant. Of course, the organization was different at that time, and I——

Mr. ROGERS. Well, it doesn't matter. Chief of security is over security over all your installations. Isn't that correct? The DOE chief of security.

Secretary PONEMAN. What I am saying is I don't know who was the chief of security in 2002, 2005, et cetera. I don't——

Mr. ROGERS. I am telling you the same guy has been there for 20 years. The guy who is the chief of security now has been the chief of security at the Department of Energy for 20 years. All of these installations fall under his responsibility. My thinking is that if a report comes out and says, we have a flawed culture of security problems at Y–12 comes out, that should have been presented to the chief of security. Now, no remedies were taken to the equipment and the other deficiencies in that system. He wasn't fired. Who does the chief of security at DOE report to?

Secretary PONEMAN. The chief of security reports to the Secretary and to the Deputy Secretary.

Mr. ROGERS. Okay.

Secretary PONEMAN. But that person, just to be clear, Mr. Chairman, does not have line authority over the sites. I am not——

Mr. ROGERS. Why not?

Secretary PONEMAN. Because that's the nature of the problem. In other words, we need to make sure that the line of authority runs straight down through the——

Mr. ROGERS. Who is responsible for establishing line authority within the Department of Energy?

Secretary PONEMAN. The Secretary.

Mr. ROGERS. Was he fired?

Secretary PONEMAN. No, sir.

Mr. ROGERS. I recognize the gentleman from Tennessee, Mr. Cooper, for any additional questions he may have.

Mr. COOPER. Thank you, Mr. Chairman.

I think we are talking about HSS.

Secretary PONEMAN. Yes.

Mr. COOPER. The Office of Health, Safety, and Security. I think we are talking about Glenn Podonsky, who has been there some 29 years. I was interested in Mr. Podonsky, as you point, because of a news article dated February 22, 2013, just a few days ago, in which he said—at least he is quoted in the article as saying—he believes that the nuclear arms complex operated better while directly under the Energy Department's defense programs prior to the nuclear agency's formation in 2000. And I think by the nuclear agency, he means NNSA. And I am not faulting Ms. Miller, because she is acting and new, but this is a pretty amazing charge from somebody that you praise and trust. And he might not have line authority, but has been there a long time, knows a lot of stuff, you all rely on his viewpoint a lot, and he is wondering whether NNSA should even have jurisdiction here.

Secretary PONEMAN. That obviously——

Mr. COOPER. And we have taken a step backwards since 2000.

Secretary PONEMAN. Yeah. Obviously, Congressman, that does not reflect the view of the Department of Energy. We clearly believe that the structure of having NNSA as the semiautonomous

part of the Department is the right structure. We are fully on board with that, and there is no question about that. I also was not present, I saw the news reports, obviously, but that is not obviously reflecting the view of the Department.

Mr. COOPER. Well, let's forget politics for a second and the view of the Department, because right now the Department doesn't have a lot of credibility on the security issue. Here is a guy who has been a loyal public servant for 29 years who is trying to express a viewpoint, and it might be politically correct, it might not be officially, you know, supported by the top brass, but this is, you know, part of your organization that you respect and trust, this is a respected individual who is questioning even the function of NNSA. And, of course, a commission will be established to look into lots of NNSA issues anyway. This is a problem.

Secretary PONEMAN. Well, Congressman, we have, all of us, thought long and hard exactly about what the best way to do security is going forward out of this episode. We will continue to do that. We are going to take advantage of the great wisdom of the three experts. And we always encourage a continued questioning attitude and not to be complacent about where we are. We have no grounds for complacency. So we are going to keep at working as hard as we can to get this problem fixed.

Mr. COOPER. Why do you deserve the chance to keep working at the problem?

Secretary PONEMAN. I don't think, sir, in terms of anything I deserve. I am just trying to address a problem, and I feel that that is my responsibility and I am going to keep working at that as hard as I can. I don't think of it in terms of what I deserve or don't deserve.

Mr. COOPER. But in response to Mr. Turner's question earlier, it seemed like you had a hard time thinking of circumstances that might even lead to, say, Air Force levels of taking responsibility.

Secretary PONEMAN. I don't mean to imply that. I strongly believe in accountability. We took every step that we could to make sure that the problem could not recur by changing the structure, by changing the culture and taking those steps, and by holding the individuals accountable. And, again, sir, we will continue to do everything we can to earn the confidence of this committee and the American people in that measure.

Mr. COOPER. Maybe you could answer for the record what the average guard or protective force member makes when you divide out, you know, there is $175,000 going to each position under DOE leadership, how much take-home pay, how many benefits are these folks actually getting out of this amazing sum of money. They are paid like Federal judges, they are paid like Congressmen, yet these poor folks are not getting that sort of benefit.

Secretary PONEMAN. Congressman, I have not seen the math. My hunch is that that number folds in a lot of physical plant and so forth. But it is absolutely a fair question to ask, and we will get you—and I assure you it won't be 5 months, I don't know how that happened—we will get that promptly to you, sir.

[The information referred to can be found in the Appendix on page 117.]

Mr. COOPER. Thank you.

Mr. ROGERS. I thank the gentleman.

Mr. Wilson, you don't have any more questions?

The last thing I wanted to point out was last week the DOE chief security officer told a reporter that the nuclear enterprise, quote, "wasn't working badly in the 1990s before NNSA was formed," and that we should just abolish NNSA and go back to having everything DOE. But then we look back, and in 1999 a report by President Clinton's Foreign Intelligence Advisory Board said that DOE, quote, "embodied science at its best and security at its worst." Highlighting a string of recurring security problems that DOE had failed to correct in the 1990s, the Board described DOE as a "dysfunctional bureaucracy that has proven it is incapable of reforming itself."

The thing that I hope you take away from this, Mr. Secretary, is you have got to be capable of reforming yourself. I want you to recognize we are as serious as a heart attack about what has just happened here and staying after it, and we expect it to be remedied. That doesn't just mean the NNSA. That also means the Department of Energy. And we want to know specifically that you are willing to terminate people that aren't doing their job. It sounds to me like this chief security officer might be one of the folks that ought to be on your list to look at.

But we are looking for serious reforms and line responsibilities so that if—and I hope we never do have another incidence like this, but if we do, you can show us or we can see exactly who was responsible and if they were dealt with in a prompt and appropriate manner.

Secretary PONEMAN. Mr. Chairman, first of all, as I said in my opening statement, we not only accept, but we welcome working with you and this committee on these problems in exactly that dimension.

Number two, we very much agree—obviously there are continuing concerns we need to address—we completely agree that accountability is a critical part of fixing the problem. However, we don't just have a people problem. We also have a structural problem. We need to fix that. We have a cultural problem. We need to fix that. Not to say we shouldn't fix all of them. We do. We are as serious as a heart attack as well. I am just saying that we need to work on all parts of the problem: accountability, culture, clarity of lines of responsibility, authorities that go with that. And, again, with your help, hopefully we will get to the place where we never do experience this kind of episode again, because it is something that is absolutely, as we have said from day one, unacceptable.

Mr. ROGERS. Thank you.

Several members went back after the last series of votes. If there are any members who have additional questions they would provide in writing, we will keep the record open for 10 days. I would ask you if any members do submit questions to you in writing, that you respond to those in writing in a timely manner.

Thank you for your time and attention. This hearing is adjourned.

Secretary PONEMAN. Thank you.

[Whereupon, at 12:46 p.m., the subcommittee was adjourned.]

# A P P E N D I X

FEBRUARY 28, 2013

## PREPARED STATEMENTS SUBMITTED FOR THE RECORD

FEBRUARY 28, 2013

**Opening Remarks – As Prepared for Delivery**

**Honorable Mike Rogers**
**Chairman, Subcommittee on Strategic Forces**
**House Armed Services Committee**

**Hearing on "Nuclear Security: Actions, Accountability, and Reform"**

**February 28, 2013**

Good morning and welcome to today's hearing on nuclear security at the Department of Energy's National Nuclear Security Administration. This is the subcommittee's first hearing of the 113th Congress, and we place a strong priority on ensuring these longstanding problems with security are fixed.

Before we get into the hearing, I want to pause and welcome new members to the subcommittee. But first and foremost I want to recognize our ranking member, Mr. Cooper of Tennessee. I look forward to working closely with him over the next two years as we carry out the important work of this subcommittee.

With every new Congress we always have some shuffling of seats at the subcommittee level, as well as new members to the committee and to the House.

New to the Strategic Forces Subcommittee on the Republican side, I welcome:

- Mr. Coffman of Colorado
- Mr. Wilson of South Carolina
- Mr. Nugent of Florida
- Mr. Bridenstine of Oklahoma

And on the Democratic side, I welcome:

- Mr. Johnson of Georgia
- Mr. Carson of Indiana
- Mr. Veasey of Texas

I look forward to working with all of you, as well as my colleagues who are returning for another two years of Strategic Forces oversight. This subcommittee has responsibility for many big, critically important issues—and we're going to get into one of them right now.

Today's hearing is part of the committee's continuing oversight of the aftermath of the security breach at the Y-12 National Security Complex on July 28, 2012. At this point, the facts of the incident are well-established, so I won't repeat them here. Needless to say, the intrusion of an 82-

year old nun and two other men into supposedly one of the most secure perimeters in the country is astonishing and completely unacceptable. Through its hearing and closed briefing last September, this subcommittee is aware of the immediate corrective actions taken by NNSA and DOE.

Today, this hearing is focused on the broader implications of the incident, including organizational, leadership, and structural failures that enabled it to occur. Depending upon how you count them, anywhere from 6 to 10 different reviews have occurred in the past six months—some narrowly focused on the Y-12 incident, and some focused on broader security management problems. Reviews are good, but now—six months after the incident—we need to see action. And if history tells us anything, it is that the Department of Energy is not known for action.

Reviewing the testimony from our witnesses, as well as other reports on DOE nuclear security stretching back 15 years, I am deeply concerned that we've been identifying the same problems for more than a decade. And those problems remain unresolved.

For instance, a 1999 report by the President's Foreign Intelligence Advisory Board (PFIAB) said the DOE "embodied science at its best and security at its worst." Highlighting a string of recurring security problems that DOE had failed to correct in the 1990s, the Board described DOE as a "dysfunctional bureaucracy that has proven it is incapable of reforming itself." The Board recommended radical reorganization, calling for a new agency, either with some autonomy with the DOE or completely divorced from it. Congress responded by creating the semi-autonomous, separately-organized NNSA.

In 2002, a few years after the creation of NNSA, another study found the same problems. The Commission on Science and Security, led by former Deputy Secretary of Defense John Hamre, said:

> "the Department [of Energy's] continuing management dysfunction impairs its ability to carry out its science and security missions....DOE's headquarters, field, contractor, and laboratory relationships create a complicated layered structure in which assigning accountability is difficult."

Ultimately, the Commission recommended that, if security reforms are to succeed:

> "the Secretary and the Administrator of the NNSA must address basic organizational problems at DOE, most significantly confusion over line and staff responsibilities...Together with a more clearly defined chain of command, DOE needs to reduce excess layers of management staff that have built up since the late 1980s."

In 2005, an independent study of NNSA security conducted by Admiral Richard Mies found the same problems, and said 8 years ago that they "are not new; many continue to exist because of a lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes."

Those reports were from 1999, 2002, and 2005.

So where are we at today? To anyone paying attention the answer is undeniably: nowhere. The assessments done after the Y-12 incident show that the exact same fundamental problems remain.

Asked by the Secretary of Energy to do an independent assessment, Dr. Richard Meserve noted in December that:

> "part of the challenge in providing proper oversight may relate to the extraordinarily complicated administrative structure within DOE, with security responsibilities spread across several offices at headquarters and between headquarters and the DOE field offices."

One of our witnesses, Major General Don Alston, drily noted in his letter to Secretary Chu that:

> "study of a variety of DOE and NNSA organizational charts could not demystify where authority [for security] lies."

Another of our witnesses, Brigadier General Sandy Finan, made similar findings, reporting that:

> "there is no clear line of authority within the NNSA security organization…Absent clearly defined lines of the authority, many individuals assert authority, while correspondingly few have been assigned responsibility."

I have an organization chart here from a 2009 report called "Leveraging Science for National Security," where yet another independent study tried to understand the lines of authority within DOE. I credit the authors for even trying to make sense of it via a diagram. Without objection, I'd like to enter this for the record.

I understand that NNSA has created a new office, NA-00, that it believes will help clarify security responsibilities. But I also understand that the other security offices, including NA-70 and the Department of Energy's Office of Health, Safety, and Security, will remain in place and likely grow in size. I am curious how the creation of yet another office within DOE Headquarters will create clarity in roles and responsibilities and simplify an already bureaucratic chain of command.

Regardless of the structural issues, there is also a problem of accountability. Based on a letter from Secretary Chu on January 31 (which I will also enter into the record), the only people who have been fired as a result of the Y-12 incident are a few guards and perhaps a few contractor employees. But no federal officials have been fired. Some NNSA site and Headquarters security officials have been "reassigned" to other positions within DOE or allowed to retire—but not fired.

Tellingly, the Department of Energy's Chief Security Officer is still in place—and is being asked to implement solutions to a dysfunctional security management system that he has presided over for 10 years. This is happening despite the fact that his organization performed an independent inspection of Y-12 only two months prior to the incident and gave its security effectiveness a resounding endorsement.

Further, a press report last week quotes this senior DOE security official saying that prior to creation of NNSA, when the nuclear weapons complex was still a full part of DOE, he believes "it really wasn't working badly." This is either revisionist history or a terrible memory, because we remember the long series of security failures in the 1990s that caused that independent board to call DOE in 1999: "security at its worst" and "a dysfunctional bureaucracy that has proven it is incapable of reforming itself."

This isn't accountability—it is deplorable. Indeed, it is the exact opposite of what Secretary of Defense Gates did after the Air Force's nuclear security problems in 2007 and 2008. His demonstration of accountability in the Air Force's senior-most leadership is my example of firm accountability—and it should be everyone's.

Last year, this committee put forward a set of proposals to fix the longstanding, well-documented governance problems at NNSA and DOE that were a contributing factor to this security incident. We are still waiting for the Administration to put forward its own proposals for reform—I am curious if and when we will see them.

But one thing should be clear by now: the status quo is not working and must not be continued. Security of our nuclear weapons is at risk, as is the NNSA mission of sustaining our nuclear stockpile. Dozens of reports and other indicators have shown that the system itself is broken, in addition to leadership, management, and personal failures. I will say to Ranking Member Cooper, and all of my colleagues, I am here to work with you to fix this broken system. It would be a crime if we find ourselves here next year and nothing has changed.

We look forward to the hearing the recommendations of the congressional advisory panel created by Section 3166 of the FY13 defense authorization act. But we cannot wait a year to start making progress. This subcommittee is soliciting all ideas regarding how to go forward, and will continue to push the system to make the changes that are so obviously needed.

Our first panel of witnesses will help us do that. They are each the author of separate independent assessments of the Y-12 incident or broader security issues at DOE and NNSA. We hope they will elaborate on their findings and recommendations, and give us a deeper understanding of the problems and potential solutions. The witnesses are:

- **Major General C. Donald Alston, USAF (ret.)**
  Former Commander, 20th Air Force
  Former Air Force Assistant Chief of Staff, Strategic Deterrence and Nuclear Integration

- **Brigadier General Sandra E. Finan, USAF**
  Commander, Air Force Nuclear Weapons Center
  Former Principal Assistant Administrator for Military Applications, National Nuclear Security Administration

- **The Honorable Gregory H. Friedman**
  Inspector General
  U.S. Department of Energy

Thank you to our witnesses for appearing today, I'm looking forward to our discussion.

With that, let me turn to our Ranking Member, Mr. Cooper, for any opening comments he would like to make.

###

**Opening Statement**

**Strategic Forces Subcommittee Hearing**
**Nuclear Security: Actions, Accountability, and Reform**

**Ranking Member Jim Cooper**
**February 28, 2013**

I would like to join Chairman Rogers in formally welcoming new members to our committee and I look forward to working with all of our members for a productive 113th Congressional Strategic Force Subcommittee. There is much work to be done.

Following up on efforts to delve into the response to the inexcusable security lapse at Y-12 which occurred last July.

I look forward to examining what security reforms are warranted, what risks must be addressed, and how to increase performance and accountability of contractors and federal overseers. We must fix this broken system.

I join the Chairman in welcoming General Alston, General Finan and Inspector General Friedman to share their insights on what the deficiencies were that led to such a debacle, and must change. I would also like to welcome Deputy Secretary Dan Poneman and Deputy Administrator Neile Miller back to our Subcommittee to help us understand the implementation of a path forward.

The July 28 intrusion by three peace activists, including an 82-year old nun, Megan Rice —who is with us here today—was historically unprecedented. They were able to penetrate, without being intercepted, 4 perimeter fences, at what is expected to be one of the most secure sites in the world.

We owe it to the taxpayers and the security of our country to require oversight that ensures effective performance, accountability and responsibility.

First, the contractors' abysmal performance was evident at every level. We spent over $150 million at the site last year for security in addition to funding for security upgrades. What we got were broken cameras for months, security guards unaware of which cameras were down,

guards dismissing alarms, and a security force unable or unwilling to follow security procedures in their response. In the aftermath of this failure, the Department of Energy discovered that the security personnel were cheating on inspection tests. The security culture was a joke.

Yet, B&W, which chose to ignore broken cameras for months and delay maintenance work that would have decreased the false alarm rate, received an "excellent" rating for its Safeguards and Security work, and received $51 million in incentive fee for FY 2011. Even more baffling, after the intrusion, B&W still received nearly 60% of its award fee—about $36 million—and was only docked $12 million for poor security performance. How are we raising accountability and liability in the contracts? Has NNSA or DOE tried to recover some of the money paid for security since the contractors failed in their performance?

Second, the federal oversight process embraced a "hands-off" approach, allowing contractor incompetence and abdicating effective oversight responsibility:

At the NNSA level, NNSA site officials, despite knowing about several of these deficiencies, failed to force the contractors to take much-needed corrective actions despite problems persisting for months. The DOE IG report found that "federal officials [stated] that with the advent of NNSA's contractor governance system (Contractor Assurance System), they could no longer intervene (…) to address growing maintenance backlogs" and that "while federal employees knew of problems at the contractor level, they perceived that the contractor governance approach prohibited them from intervening in contractor activities." This lack of oversight had disastrous impacts on security readiness, as has become evident.

With regard to DOE: because of concerns of excessive and overly burdensome oversight, the Department of Energy streamlined and eliminated many DOE safety and security directives despite concerns from GAO and the Defense Nuclear Facilities Safety Board. The GAO noted in April 2012 "that the benefits of this reform are unclear because the DOE did not determine if the original directives were in fact burdensome and the reform did not fully address safety concerns."

In addition, with support from the contracting community, DOE loosened contractor accountability by revising executive order (DOE Order 227.1) related to tracking corrective actions to address deficiencies identified by the independent Health Safety and Security Office.

While we must reduce bureaucracy, DOE and NNSA must strike a workable balance to maintain effective oversight.

Meanwhile, DOE's Office of Independent Oversight staff conducted inspections only every few years and lacks the responsibility and any enforcement mechanism for ensuring that problems identified in independent assessments are corrected. This responsibility resided with NNSA site offices which did not feel empowered to demand performance from contractors.

Independent oversight done by qualified and experienced experts remains a crucial element to ensure the security of sites with nuclear weapons-usable material.

Thank you for your insights on the root cause of this completely unacceptable failure, and I look forward to hearing what NNSA and DOE are doing to fix it, and how Congress can help ensure we make meaningful change.

This is too important a task and too expensive a mission to fail. We've had a real wake-up call. It is our responsibility and we cannot get this wrong under our watch.

Thank you Mr. Chairman.

**Statement before the U.S. House of Representatives**
**Committee on Armed Services**

**Subcommittee on Strategic Forces**

# Hearing on

# Nuclear Security:

# Actions, Accountability, and Reform

**A Statement by**

**C. Donald Alston**

**Major General, USAF (retired)**

**February 28, 2013**

**Rayburn House Office Building Room 2212**

Nuclear Security:
Actions, Accountability, and Reform

Statement of C. Donald Alston
Major General, United States Air Force (retired)
Before the Subcommittee on Strategic Forces
of the U.S. House of Representatives Committee on Armed Services

February 28, 2013

Mr. Chairman, Ranking Member Cooper, members of the subcommittee, I thank you for the opportunity to appear before you today as part of this distinguished panel.

With the subcommittee's permission, I would like to submit as my statement three separate letters, authored by Mr. Norman Augustine, Dr. Richard Meserve, and me, which we provided to Secretary of Energy Dr. Stephen Chu in support of our examination of physical security at Department of Energy Category 1 nuclear facilities. In October 2012, Secretary Chu asked the three of us to consider a variety of security models and to provide our separate, individual observations regarding any emerging constructs that may be viable for application across Department of Energy and, specifically, National Nuclear Security Administration sites. We provided our respective letters to Secretary Chu on December 6th of last year.

I would also like to provide some additional context about our assessments for the purpose of clarity. While Secretary Chu did not ask us to investigate the Y12 security breach in particular, we used that incident and resulting investigations as an entry point into a larger examination of the physical security construct. Additionally, we were exposed to draft corrective actions resulting from those investigations, but we did not evaluate these measures or their implementation across Department of Energy and the National Nuclear Security Administration. Finally, our written assessments were informed by our direct engagement during a brief seven-week period last fall, culminating in early December.

Mr. Chairman, Ranking Member Cooper, and members of the subcommittee, below are letters to Secretary Chu from my esteemed colleagues and me. Thank you for the opportunity to appear today before the subcommittee, and I welcome your comments and questions.

C. Donald Alston
1515 North Star Loop
Cheyenne, WY 82009
December 6, 2012

The Honorable Steven Chu
Secretary of Energy
U.S Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Dear Secretary Chu:

In light of the perimeter security breach at the Y-12 National Security Complex (Y-12) in July 2012, you asked me to examine a variety of organizational constructs for physical security and to provide you with observations on the value of transitioning to a common model.

My observations have been informed by reviewing the considerable body of work that has been done on this subject over the past decades; through interviews and discussions with current and former DOE leaders, as well as experienced leaders outside of DOE; and by a number of site visits. I was able to visit DOE headquarters (HQ), Y-12, Pantex Plant, Sandia National Laboratories, Los Alamos National Laboratory, Savannah River Site, and the Calvert Cliffs commercial nuclear power plant in Lusby, MD. The site visits enabled discussion with maintenance and operations (M&O) contractors, DOE overseers, and protective force management and members, including union leaders. A very candid exchange at all levels with dedicated, experienced professionals greatly aided the effort.

Four physical security organizational models were reviewed: 1) a proprietary protective force organic to the M&O contractor responsible for site operation; 2) a protective force subcontracted to the M&O contractor; 3) a federalized protective force; and 4) U.S. military forces. Three of these four models are currently functioning within DOE/National Nuclear Security Administration (NNSA); however, none of the four emerges as attractive long term, department-wide option without addressing systemic impediments that preclude effective change.

On the grandest scale, there were indications that security was viewed as the responsibility of the protective forces alone rather than as the responsibility of each member of the work force. While this culture may not be widespread throughout the DOE complex, it is clear that leadership could further emphasize the need to view security of our nation's sensitive nuclear materials as a shared commitment across the work force. The Department of Energy is responsible for America's nuclear enterprise, and enterprise credibility is derived from the trust and confidence our citizens, national leadership, friends, and allies have in the Department's ability to maintain a safe, secure and effective U.S. nuclear weapons complex. Importantly, this credibility factors into the daily calculus of potential adversaries and contributes directly to achieving an effective deterrent posture, a commodity re-earned every single day. A pervasive culture in which each member of the nation's nuclear weapons complex recognizes the vital role he/she plays in assuring both security and safety contributes directly to maintaining that credibility.

As currently structured, no recognizable critical path exists between DOE HQ and the site security organizations to ensure daily security success. Study of a variety of DOE and NNSA

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

organizational charts could not demystify where authority lies. The Department struggled to articulate how information flows – both up and down – between the sites and DOE HQ and could not easily provide a depiction of that process. I think this environment contributes to the reality that nuclear material at Savannah River Site – which falls under DOE's Environmental Management (EM) office – can be secured with different standards and policies than those required at NNSA sites. The category of material should drive security requirements, not the organizational chart.

Distance has been growing between the headquarters and the sites, a trend that follows a DOE legacy of decentralized management across its facilities. While this traditional arrangement may pay dividends for the department in many respects, security is not one of them. Recent efforts to revise DOE's safety and security directives and modify the department's oversight approach to provide contractors with the flexibility to tailor and implement safety and security programs without excessive federal oversight or overly prescriptive departmental requirements, as well as NNSA's "governance transformation" that increased reliance on contractor's self-oversight through its contractor assurance systems, have fortified sites' sense of independence and distance from the HQ. Sites leverage their unique missions and geography to justify a preferred "alone and unafraid" mantra, and the HQ has employed a largely "hands off" response.

Mutual distrust is bred as HQ personnel in key security roles are viewed as inexperienced regarding security matters and too far removed from the site to understand the uniqueness of local challenges. Key leaders must have credible security experience -- especially since there is little to no assignment circulation of security personnel to and from the HQ; no missionaries emerge to bridge the gaps in trust.

What little leverage the HQ has comes in the form of additional inspections and assessments – "black hat" interactions that further contribute to adversarial relationships. Inspection is an absolutely essential tool to validate compliance and operational readiness. However, it should be one dimension of a composite assessment process. Depending too much on snapshot assessments and not developing the right metrics to measure daily readiness would provide leadership little satisfaction regarding the true state of security preparedness and program execution.

Further, there is a perception that corporate security policy is being written from inspection results. If true, the Department risks drifting from measuring original standards to an environment where sites lack confidence in the integrity of the inspection process as they perceive they are chasing the latest inspection results. In the DOE/NNSA HQ construct, a dynamic or volatile policy environment led by DOE's Office of Health, Safety, and Security (HSS) risks marginalizing NNSA security responsibilities. Of course, even if these site perceptions are inaccurate, leadership needs to be sensitive to these atmospherics.

Communication is an area ripe with opportunity. Given today's environment where sites seem to prefer to operate independently, where there is no effective best practice/lessons learned dialogue between sites, no program for security information exchange with the Department of Defense (DoD) or commercial nuclear activities, it is not surprising that site facility staffs can and do conceive, design, develop, test and deploy modifications to security systems. To better understand and share risks associated with changes to security systems there could be a normalized process over watched by DOE HQ, leveraging a revitalized Sandia expert review, with hard requirements for developmental and

operational testing and red teaming that could methodically deliver security modifications ready on day one.

In my final analysis, the NNSA Administrator must always be able to answer the following questions:

- How ready are we today and how do we know?
- How ready will we be in 6 months and how do we know?

A variety of sources produce the set of ingredients that create the mosaic of indicators conveying the current and future state of the security program. Timely, balanced reporting, where good news travels fast and bad news faster, not only provides content, but also serves as a barometer for the quality of the self-critical culture. Quality metrics that provide both tactical and operational level content, deliver today's picture and, measured over time, expose trends and opportunities for course corrections. Collaboratively developed metrics, together with processes that actively seek input where appropriate on policies and standards also builds trust. Checks and balances in development of new or improved security capabilities, to include external review processes, provide corporate-wide awareness and ensures sites have support during transitions. A comprehensive human capital development program creates career paths at all levels and could provide for circulation up and down the chain, all the while driving greater security competency across the enterprise.

Based on discussions over the past two months, the attributes of the objective security organizational construct should include:

1) A force with a mission focus that understands the vital interdependencies and coordination required at all times with the M&O contractor;

2) A well-trained, disciplined force whose professional conduct during routine operations is dependable and above reproach and one that is prepared to use lethal force if required during emergency operations;

3) A force conditioned and incentivized by leaders at all levels to provide timely reporting;

4) A force that would help drive crosstalk across DOE sites, outside the department such as with the DoD, and with commercial nuclear businesses to benefit from others' lessons learned;

5) A force with an absolute intolerance for compensating for shortfalls/deficiencies/outages one minute longer than necessary;

6) A force that knows - based on facts -- how ready it is today and leaders who know how ready it will be 6 months from now;

7) A force not remotely prone to work stoppage as a job action; and

8) A force that understands the merits of centralized control and decentralized execution of security responsibilities.

Of all the candidate security organizational models I examined, the military model is the least attractive to me to meet DOE/NNSA needs. The advantages include a dependable, high-quality, rotating force that would routinely be refreshed to meet mission demands of a typically non-dynamic environment. However, the lack of continuity would produce a force less familiar with the site than other models, and transitory leadership will have to adapt to a relatively unfamiliar mission (enriching uranium, for example). The most significant disadvantage is the division of unity of command by the introduction of a substantial command and control seam between protective forces and site operations with the arrival of Department of Defense onto the DOE/NNSA playing field. Would there be any risk that geostrategic instabilities might make these war fighting forces the first to be redeployed abroad, driving challenging domestic security contingency plans? I do not see an effective role for a DOE/NNSA representative in this model.

The proprietary guard force, which has security personnel organic to the M&O contractor operating the site, provides the cleanest unity of command option. The risk of security work stoppage seems less likely in this model than other contractor options. Poor performers can be removed with ease. The drawback to this option is the uncertain security competencies of potential M&O contractors. This model is a variation on the status quo where a DOE/NNSA security representative provides oversight of the security elements of the M&O contract.

The model in which the protective forces are part of a company subcontracted to the M&O contractor has a mixed record. There is a history of work stoppage. There is a manageable seam as far as unity of command is concerned. History shows this model can provide a disciplined, professional force with valuable continuity and familiarity with the site. (I would note here that military experience probably makes up between 50 and 75% of the force, though most of those veterans have no nuclear security experience upon arrival. Good orientation and training programs make up for this significant deficiency and ensure those with and without military experience are prepared to provide effective security.) At Y-12, the maintenance function was not owned by the protective force which may have contributed to improperly prioritized maintenance of security gear, which ultimately resulted in failure. Overcome this specific contract deficiency and this model will present less risk than it currently does. This model is a variation on the status quo where a DOE/NNSA security representative provides oversight of contract execution by the sub-contractor.

The model I find the most attractive is the federal model. It is proven, working effectively in the DOE/NNSA transportation business providing for a disciplined professional force. It precludes work stoppage risk. True, adverse actions are less swift than the contractor models and this approach does introduce a seam with the M&O contractor. However, this model is a substantial departure from the status quo and what you trade in local unity of command you gain in more effective corporate oversight of security operations. I see the role of the DOE/NNSA security representative as the leader of the site security forces and the key integrator with the M&O leadership. The long term culture shift this model could drive should be weighed positively in an organizational change decision.

For your consideration, Admiral Mies oversaw an in-depth study of DOE security in April 2005, "NNSA Security: An Independent Review." I think a hard-hitting, 'show me' re-assessment of the status of his recommendations would benchmark the state of your self-critical culture and prove very helpful to the Department.

All members of your Department rapidly responded to requests for information and made time for discussions at my convenience. Everyone I met, both the contractors and Department personnel, were forthright, professional, and dedicated to mission success.

I am honored you asked me to support this important project. Thank you. It was a great experience working with the men and women of your Department. And thank you for providing the support of the talented members of Center for Strategic and International Studies. I could not have produced this work without their tireless support.

With great respect,



C. DONALD ALSTON

**NORMAN R. AUGUSTINE**
**6801 Rockledge Drive**
**Bethesda, MD 20817**
**Tel. 301-897-6185 Fax 301-897-6028**
**norm.augustine@lmco.com**

December 6, 2012

The Honorable Steven Chu
Secretary of Energy
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Dear Mr. Secretary:

This letter responds to your request that I assess certain physical security shortcomings experienced by the Department of Energy (DoE), most prominently at the Y-12 National Security Complex (Y-12), and provide observations, findings and recommendations.

Given the relative short amount of time available for this review, my recommendations are more in the form of suggestions; however, they are based on over a half-century of managing at all levels in large organizations. I have drawn upon lessons gained during the ten years I devoted to government service, including several years as Under Secretary of the Army, and a number of years as CEO of an organization with over 180,000 employees, many working on sensitive national security systems. Further, in keeping with your request, I have been extremely candid in my assessments, which in no way suggests any diminishment in my overall respect for the people who are charged with such enormous responsibilities as are those in your Department.

Although this letter is no doubt considerably longer than you intended, the matter at hand is in many respects a complex one, and its importance obviously merits careful consideration. This document has been prepared at the unclassified level for your convenience; however, I would be pleased to provide further substantiation and clarification of various issues at a higher level of security, should you wish.

I would note at the outset that I am highly indebted to the people working in the Department of Energy, who were generous with their time and expertise and were extremely forthcoming, even welcoming, in sharing their views on what are often controversial issues. A particular debt of gratitude is owed to the staff of CSIS that supported us; they are a group of professionals.

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

**APPROACH**

In conducting this review, I have read on the order of 1,000 pages of documents, some at classified levels, and held discussions with literally dozens of individuals, both management and non-management—the latter in some cases without management present. I visited Y-12, Pantex Plant, Sandia National Laboratories, Savannah River Site, DoE headquarters, and the Calvert Cliffs nuclear power generation plant. (The reason for conducting the field visits was to benefit first-hand from examining the different management models they embrace; to search for systemic problems; and to assure the degree of thoroughness that the task you assigned deserves.)

The mindset you will hopefully find reflected in this letter is one commensurate with DoE's extraordinary responsibility of, among other things, providing for the security of sensitive nuclear materials and weapons. Failures in this arena can, as you know so well, directly impact the lives of millions of people as well as reshape the world's geopolitical landscape virtually overnight. Under such circumstances, there can be zero margin for error, and that is the attitude that has been adopted in conducting this review.

**OVERALL FINDINGS**

"Unacceptable and inexcusable" were the words aptly used by the Administrator of the National Nuclear Security Administration (NNSA) testifying before the Congress with regard to the events of July 28 at Oak Ridge; as you know, three individuals, one an 82-year-old nun, penetrated four fences and several clear-zones during the night, and when finally confronted, these individuals faced a trained security officer who acted principally as a spectator. Disconcertingly, I can see little reason why, under the specific prevailing circumstances, the intruding group could not have included, in addition to the three persons actually participating in the incursion, a well-armed follow-up group. I must disclose that I have been involved in dozens of failure analyses of a variety of types during my career, and none has been more difficult for me to comprehend than this one.

Many security professionals with whom we spoke reacted to the Y-12 incident with extreme embarrassment and, as in my own case, perplexity. The overwhelming majority of these individuals are very proud of the work they perform and are generally aware of the importance of their mission…which makes the cascade of failures that led to the events of July 28 all the more enigmatic.

You asked that I address the pros and cons of various management structures that would better serve the Department in providing physical security, and I have done so. While this is important indeed, I conclude that, rather convincingly, the management structure was an abetting, not a root cause, of the problems encountered on July 28. The fundamental

problem was one of culture: a pervasive culture of tolerating the intolerable and accepting the unacceptable.

As examples of this culture, a false alarm rate surpassing by orders of magnitude anything that I have ever encountered before was accepted as a fact of life. When full-time surveillance cameras failed, a "compensatory measure" was introduced that consisted of (relatively infrequent) periodic patrols. Word of no-notice tests was leaked to those security forces being tested. Failed security systems went unrepaired for months (yet were repaired within days after the Y-12 incursion when attention was focused upon the issue). There was cheating on proficiency exams. "Tune-up" firing was permitted prior to marksmanship qualification tests. Worthiness tests of hardware were delayed until the hardware was in working condition on the grounds that there is no sense testing hardware that isn't working. Strikes of the guard force were largely dismissed as being readily offset by substitute guards (even though we were told that as many as three sites have entered union negotiations at about the same time, which could limit the availability of such substitutes).

The demands of securing nuclear materials, components, and devices are perhaps of unmatched unforgiveness—yet in general it is an endeavor of chilling monotony. Individual security personnel can (hopefully) expect that they will never confront a true threat during their entire career. Add to this the hundreds of false and nuisance alarms that occurred (and occur) each month—and then working 12-hour shifts (albeit some involving rotation)—and one has a mind-numbing challenge even for the most dedicated professional. (Regarding the length of shifts, as explained in one DoE report, the workforce likes the overtime pay and days off.)

The various corrective action plans and numerous security reviews (going back to 1986) reveal a pattern of inverted priorities, to wit, from highest to lowest:

1. Accommodate the workforce.
2. Reduce costs.
3. Secure nuclear materials, components and devices.

In summary, the problem the Department faces within the context of this review is a culture of permissiveness, amplified by the absence of day-to-day accountability and exacerbated, in the case of Y-12, by an ineffectual governance structure.

As will be discussed later, I favor the Federalized Force model for a number of reasons. However, if this cannot, for various reasons, be implemented, I believe that the single-contract ("new" Y-12) model can be made to work…as could another alternative I will offer.

Unfortunately, one of the most difficult things to change is a failed culture. My observations over the years have, however, convinced me that change can be introduced and that there are at least seven ingredients to successfully do so:

1. Make sweeping changes...begin with a "clean sheet of paper"—simply "trying harder" to do what you have been trying to do all along is a formula for failure.
2. Make leadership changes wherever doubts exist as to its effectiveness.
3. Devote a great deal of effort to communicating the new culture.
4. Be intolerant of even the slightest reversions to the old culture.
5. Lead by example—demand that all in leadership positions *"walk the talk."*
6. Execute change fast...prolonging change so that everyone can get used to the new system is self-defeating.
7. Weed out individuals who cannot accept the new culture (Vince Lombardi: "If you are not fired with enthusiasm you will be fired with enthusiasm!")

**CAUSAL FACTORS (Y-12)**

The following six factors seemed to predominate as triggers for the Y-12 incident of July 28 (note: one earlier assessment identified 26 specific factors that contributed to the security failures):

**Failure of Early Warning System**. Numerous reviews of Y-12 physical security have been conducted over the years; however, none—including one by NNSA not long before the July 28 incident—expressed extraordinary concerns, although several cited troublesome indicators. In the case of the line-management system, the headquarters relied upon the site management; the site management relied upon the two primary contractors; and one of the two primary contractors was facing a competition and the union was concerned with an upcoming contract negotiation. In short, bad news did not flow upward, having been underappreciated or filtered at every level. The speed of light exceeds the speed of dark!

**Lack of Systems Approach**. Razor (or concertina) wire was in place around part of the Y-12 perimeter...but not all. There was no evidence of a disciplined analysis of single-point or even multi-point failure modes. DoE sites, for example, have far fewer cameras than does the Calvert Cliffs power plant. It was reported that sixty compensatory measures were in place at Y-12 to "offset" malfunctions, but from a systems standpoint many of them were not truly compensatory. When the necessary funding to implement the ARGUS security system was not forthcoming (by nearly a factor of four), ARGUS was mated to elements of the existing system without adequate systems testing—and then rushed into

operation—apparently without objection by the Site Office. The result was that the "system upgrade" actually deteriorated system performance.

**Split Responsibilities**. Wackenhut Services, Inc. (WSI) was responsible for the security force but the management and operations (M&O) contractor was responsible for the sensing, analysis, and display equipment. The Site Office appears to have withdrawn from its oversight responsibilities, having misinterpreted headquarters instructions as to its role. The role of a Site Office (or headquarters) with regard to contracted activities is not to manage those activities but rather to ensure that those activities are managed. At Savannah River Site, physical control of category 1 materials located at two proximate sites is currently overseen via two different chains of command emanating from DoE headquarters.

**Focus of Inspection/Testing on Compliance**. In general, inspections and testing have focused on verifying that contract terms are satisfied or that the Design Basis Threat (DBT) has been countered. Immense volumes of documentation containing innumerable check-lists have been produced—little of which addresses what the Department of Defense would consider Operational Testing (as opposed to Developmental Testing). Stated differently, tests have too often addressed the question, "Does the hardware or practice meet the design criteria rather than is it operationally effective?" Standards are often procedural rather than performance-oriented, and stress testing has been lacking. What is needed is not more inspections but better inspections.

**Compartmentalization of Responsibility**. During the review team's visit to the Calvert Cliffs nuclear power plant it was emphasized that if, for example, a member of the security force noticed that a production machine sounded differently from what they normally heard they would view it as their responsibility to report this observation. Further, it was the clear responsibility of management to run the apparent anomaly to ground and to report their overall findings to the security officer initially reporting the issues. This is in stark contrast to what occurred at Y-12.

The fact that certain sensors at Y-12 had been designated as priority 2 for repair should not have been an excuse for a very large number of sensors remaining inoperable for months, particularly when the problem was not elevated within the management structure, particularly including the Site Office, for resolution.

During visits to the previously listed sites, one heard complaints about persistent escapements (deficiencies) that were known and accepted because "That belongs to the M&O contractor," "It is part of the union agreement," "It is required by the contract," "The FAA wouldn't like it," "You can't cut down trees," etc. It is critically important that all escapements be identified and reported, resolution responsibility assigned, root causes found, corrections introduced and tested, and open-items formally closed. (In this regard,

NASA and its contractors have evolved highly effective systems in support of the human spaceflight program that might be conceptually helpful to the DoE.)

**Lack of Independent Verification.** Testing and auditing ultimately requires independence from those responsible for what is being examined. At some point these two functions obviously must come together in the chain of command; however, in general, the higher that coincidence takes place, the better. This is particularly true of operational (performance) testing that may involve off-nominal conditions.

The key individuals involved in such independent oversight need to be rotated periodically, much as audit firms are required to rotate account managers or the NRC rotates its field personnel. Absent this, the site offices can become relatively passive and increasingly insular. Site managers must be granted significant authority (and accountability) over work performed by contractors—not to give detailed instructions regarding work execution but rather to assure that contractor responsibilities are being met. Similarly, headquarters personnel should not seek to involve themselves in the actual execution of routine work, but should use their full authority to ensure that significant work is in fact properly executed. In short, micromanagement on the one hand and passivity on the other are not the only options.

**MANAGEMENT PRINCIPLES**

The suggestions that follow are driven by twelve management principles that I have discerned over my career (some the hard way!). These are as follows:

1. Recognize that management is all about people. Selfless, competent, committed, ethical leadership-by-example is the coin of the realm.
2. Focus on the primacy of mission.
3. Communicate expectations and listen to concerns. Establish a single chain of responsibility and provide commensurate authority and resources.
4. Maintain clear—and minimal—interfaces (both technical and organizational).
5. Assure accountability and enforce consequences.
6. Disproportionately reward significant contributors and do not endure under-contributors.
7. Analyze every escapement—no matter how trivial—to determine root cause, introduce appropriate corrections, and conduct confirmatory tests. ("There is no such thing as a random failure.")
8. Provide independent checks and balances.

9. Maintain parallel channels for surfacing bad news (line management, auditors, ethics officers, suggestion boxes, etc.).
10. Culture can be an asset but it can never be an excuse.
11. Treat all persons with respect.
12. Operate ethically at all times.

Quality personnel can make up for an inadequate organizational structure, but a quality organizational structure can never make up for inadequate personnel.

**ALTERNATIVE MANAGEMENT STRUCTURES**

The myriad possible governance and management structures can conveniently be grouped into five basic models or hybrids thereof. Each has its advantages and disadvantages and, interestingly, three of the five are currently in use by the DoE, thereby offering first-hand experiential prototypes. These models are (a) Dedicated Physical Security—Military; (b) Dedicated Physical Security—Civilian; (c) Separate Operations and Physical Security; (d) Separate Operations and Full-Service Security; and (e) Integrated Operations and Physical Security.

*(a) Dedicated Physical Security—Military (Department of Defense (DoD))*
This model has the advantage of resolving protective force career issues, promoting strong discipline and providing a single, established chain of command. It suffers from coordination issues that may arise between two major government departments (DoE/DoD), rapid turnover of personnel, and a visibly expanded operational role of the uniformed military within the United States. Furthermore, assigning such a mission to DoD, even given its importance, would inevitably be viewed as a distraction from the Department's primary mission—a mission that is already extremely strained due to growing resource limitations.

*(b) Dedicated Physical Security—Civilian (DoE Office of Secure Transportation - OST)*
The option of a federalized physical security force would virtually eliminate concerns over work stoppages, increase continuity, and offer a clear and highly focused chain of command. It also recognizes the paramilitary—as opposed to civilian—nature of defending nuclear assets. However, it poses career management challenges for the members of the force as they age, and it has been asserted that it could be more costly than some other options. This approach represents a transformational change that should promote creating a new culture; however, it would be very difficult to "unwind" if it should later be desired to do so. (Under this model it is important that the Dedicated Physical Security Force have an integral capability to install and maintain all security systems as well as to access

organizations capable of developing such systems so that interface issues similar to those encountered at Y-12 are to be precluded.)

*(c) Separate Operations and Physical Security ("old" Y-12))*
This model can produce significant potential interface challenges (between the M&O contractor and the security contractor) because of split responsibilities and reporting chains. It is also subject to work stoppages. On the other hand, it offers the advantage of a direct relationship between the Site Office and the critically important physical security contractor and greatly eases the problem of removing non-performing individuals and organizations.

*(d) Separate Operations and Full-Service Physical Security (new model)*
The primary failing of the Separate Operations and Physical Security model that was previously in place at Y-12 is its split of responsibility between two contractors for the performance of the physical security function. A workable excursion from this model that would maintain the needed emphasis on physical security professionals who are directly aligned with the Site Office would be to have separate M&O and physical security contractors *but with the latter having a "full-service" responsibility.* That is, the security contractor would be responsible not only for providing the Pro-Force but also for acquiring, installing and maintaining all security systems and other necessary equipment—directly overseen by the Site Office. In other words, rather than moving the Pro-Force to the M&O contractor, move that part of the M&O contract related to physical security to the security contractor. This would likely exacerbate relationships between operating employees and security employees but would provide a strong physical security capability and would remove physical security responsibilities from the M&O contractor that is more likely to be familiar with science or operations than physical security.

*(e) Integrated Operations and Physical Security ("new" Y-12, Pantex)*
At the M&O level, this model unifies responsibilities for security and operations and provides the site office with a single point of contact. It also permits rapid resolution of personnel and major contractor issues. It suffers from the possibility of work stoppages and demands that the M&O organization and its senior members assume a breadth of responsibility that spans from plant operations to maintenance to cyber security to physical security and much more. Most potential M&O contractors will not be versed in the demands of providing physical security. The formation of joint ventures alleviates this problem but does not eliminate it. In the case of sites focused on research and development it confronts the challenge of integrating the open culture of science with the closed culture of security. Particularly in time of crisis the M&O contractor, security contractor and Site Office will need to maintain close coordination; however, this is not unique to this

particular model since in all cases under such circumstances operational command shifts to the Pro-Force, with other organizations assuming a supporting role.

**SUGGESTIONS**

Given that no single model seems to offer a perfect solution, I would rank the five principal options, from best to worst, as follows, with the fourth of these being undesirable and the fifth being unacceptable (note that the second and third of these options would be considerably more attractive were it possible to obtain a federal ruling/law that precluded strikes by employees of commercial firms charged with securing Category 1 sites):

- Dedicated Physical Security—Civilian ("Federalized")
- Separate Operations and Full-Service Physical Security ("New Model")
- Integrated Operations and Physical Security ("Proprietary"—"New" Y-12)
- Separate Operations and Physical Security ("Old" Y-12)
- Dedicated Physical Security—Military (DoD)

The above ranking is, curiously, somewhat contrary to my confessed personal prejudices—that is, believing that the Free Enterprise System does work and that government should perform only those functions that the private sector cannot, or will not, perform (there are of course a number of such functions). However, in the case at hand, an overriding consideration is that the DoE is concerned with one of the most consequential missions in the world; furthermore, it is a paramilitary mission potentially entailing the use of deadly force. Such a mission is best executed with a singular focus and with the greatest possible authority.

The notion that individuals under some other models, many of whom have served our country in combat, would abandon their posts in a work stoppage while protecting a Category-1 site is, frankly, incomprehensible to me. Whatever the case, the federalized model largely negates that happenstance. I discount the rather widely-held view that such eventualities are readily handled through backup plans, and do so in part because of the possibility that (as has recently occurred) multiple union contracts could expire at about the same time. (Note that work stoppages become a possibility even when union contracts contain no-strike provisions *if that contract is no longer operative due to its expiration.*)

It is again emphasized that the Dedicated Physical Security—Civilian model must be a "total package" solution and include an integral capability to obtain and maintain all necessary physical security devices and equipment.

There are at least two major disadvantages to this overall approach. First, it poses non-trivial challenges in workforce career management. Second, any attempt to implement it is likely to confront enormous opposition. With regard to the former, it is noted that there

are many government jobs (as well as M&O contractor jobs) that security force members can fill when they are no longer capable of meeting the high physical standards demanded when assuring nuclear security. Further, during the review, few if any instances were found where such problems have been significant (under any of the models in use). With regard to the latter concern, it is simply noted that the issue at hand has to do with the security of nuclear materials and weapons. Enough said!

If, however, for any reason it is not practicable to implement the Dedicated Physical Security—Civilian model, the Separate Operations and Full-Service Physical Security model or the Integrated Operations and Physical Security model, the latter as used at Pantex and has been introduced at Y-12 following the July 28 event, should be workable. The Integrated Operations and Physical Security model could involve either a single contractor or a joint venture. Both options offer the distinct advantage of making necessary corrective actions regarding personnel far more expedient than the preferred approach cited above. (In my experience, I have found the government personnel system to be far more tolerant of [the relatively rare cases of] clearly substandard individual performance than the civilian sector.)

The DoE is currently in the rather awkward situation of having (appropriately) abandoned as unworkable the Separate Operations and Physical Security model at Y-12, yet continuing to preserve that same model at the Savannah River Site (SRS)—with exactly the same security contractor! In discussions with the leadership of SRS it was clear that they are uniformly confident of the suitability and effectiveness of the existing situation. Based upon a one-day visit I would be hesitant to question that judgment since, as repeatedly observed herein, given capable people almost any model can be made to work. However, I would *strongly* emphasize that some models are markedly more vulnerable to problems than others. It is my view that the Separate Operating and Physical Security structure is such a model.

Other related actions that I would commend for your consideration are:

- Establish a separate, dedicated organization responsible for conducting physical security (only) inspections and audits that reports directly to the Secretary of Energy (or, alternatively, the Nuclear Regulatory Commission). Field Sites would be responsible for periodically reporting status of all security elements to this organization.
- Reinforce the authority of Field Sites and Field Offices—nonetheless making clear that during actual physical security incidents the chain of command is entirely within the physical security management structure and that Site office responsibility is not to manage work but to assure that work is managed. If the Site Offices are present merely to observe, then it is not apparent why they are present.

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

- Rotate select individuals between Headquarters and field sites in order to enhance understanding of the distinct roles, challenges and responsibilities faced by these two institutions (as is commonplace in industry) and thereby increase overall effectiveness. This will require revisions to the existing DoE policies for reimbursing the cost of employee moves.
- Place security forces on eight-hour shifts. This would have the secondary benefit of producing a larger Pro-Force pool. (This is undoubtedly a strike issue.)
- Create a single office (at Sandia or Livermore) to develop standards and procurement guidance along with advanced equipment for security systems (biometrics, high resolution displays, animal-discriminating sensors, etc.). These standardized systems can then be tailored, *by exception*, to the particular local conditions of individual sites. (It is noteworthy that not all such solutions need to be high-tech. For example, Savannah River Site has implemented what appears to be a very effective rip-rap barrier, yet it is not in evidence elsewhere (excluding the Calvert Cliffs nuclear power plant where it is fully embraced). The use of dogs is another such example.
- Review the current threat model (which is said to be five years old). Involve outside organizations from both the intelligence community and the special ops community to participate in this effort.
- Re-balance responsibilities among NNSA and other DoE headquarters entities to assure that field elements operating under similar circumstances are provided with a single, consistent chain of command and set of procedures. The creation of the reporting relationship of the Field Sites to NA-00 seems appropriate for clarity of command but will require careful implementation to avoid the evolution of "stovepipes."
- Reevaluate current training practices with the assistance of outside organizations (military special operations forces (SOF)). Possibilities range from such simple actions as increasing the number of allotted training rounds to enhancing force-on-force testing methodology. (I am aware that many of the DoE security personnel have had earlier experience with the above organizations!)
- *Change the culture!* This can be facilitated by adopting the previously mentioned practices. It is emphasized that a primary benefit of the "Federalized Force" model is that it does provide a fresh start—a "clean sheet of paper."

**CONCLUDING OBSERVATIONS**

The President's Foreign Intelligence Advisory Board (PFIAB) included the following comment in its 1999 report regarding DoE: "A department saturated with cynicism, an

arrogant disregard for authority, and a staggering pattern of denial." While I observed nothing approaching the former two criticisms, the third does have resonance, at least with operations at Y-12. The pervasiveness of this sense of denial throughout DoE's physical security system was not determinable in the time available for this review. Nonetheless, there is ample reason to thoroughly reassess the activities at other sites in search of patterns of behavior that may also require corrective action.

No matter what management model is adopted, the same individuals are likely to populate it—with the exception of a few senior managers. Fortunately, the people we met during our assessment appeared to be individually highly capable and clearly dedicated, but often overwhelmed by a culture of accommodation and passiveness when in the presence of sub-par performance. Somehow, at least at Y-12, a culture of tolerance overcame a culture of performance. And while one could never, ever condone the actions of the trespassers on July 28, they inadvertently provided a much needed wakeup-call to those responsible for physical security at the nation's nuclear facilities. And while the Y-12 trespassers could not, in retrospect, pose a meaningful threat even given the extent of access they achieved, the magnitude of the failure of the security system was extraordinary. Strikingly, there have been incidents in earlier years at Savannah River and Rocky Flats that point to much the same cultural shortcomings as have been allowed to persist at Y-12. Change is needed...and needed quickly.

I would note that a great deal of additional information resides at CSIS, and I believe it would be a sound investment for it to be compiled and provided to the DoE.

Finally, I am honored that you requested that I participate in such an important undertaking and pleased that you encouraged me to be forthright in my assessment. I hope that my comments will be viewed as constructively offered and that they might assist you and the members of your team in addressing the challenges the nation confronts in securing nuclear assets.

Norman R. Augustine

Norman R. Augustine

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

CARNEGIE
INSTITUTION FOR
SCIENCE

December 6, 2012

OFFICE OF THE PRESIDENT

**Richard A. Meserve**
rmeserve@carnegiescience.edu

SCIENTIFIC DEPARTMENTS

**Embryology**
BALTIMORE, MARYLAND

**Geophysical Laboratory**
WASHINGTON, DC

**Global Ecology**
STANFORD, CALIFORNIA

**The Observatories**
PASADENA CALIFORNIA AND
LAS CAMPANAS, CHILE

**Plant Biology**
STANFORD, CALIFORNIA

**Terrestrial Magnetism**
WASHINGTON, DC

**Carnegie Academy for Science Education**
WASHINGTON, DC

Carnegie Institution
of Washington

1530 P Street NW
Washington, DC 20005

202 387 6400 Phone
202 387 8092 Fax

Secretary Steven Chu
U.S. Department of Energy
1000 Independence Ave SW
Washington, DC 20585

Dear Steve:

I am writing in response to your request for advice on the management of physical security at the facilities with Category I material under DOE control. You have explained that this request arose as a result of the event at the Y-12 Highly Enriched Uranium Materials Facility in July in which three people, including an elderly nun, were able to penetrate the security fences and to deface the exterior of the building before being apprehended. In addition to this troubling breach, the first responder's casual behavior upon encountering the intruders was completely inappropriate given the nature of the site.

The security challenge confronting the Department is a complicated one for a variety of reasons. The DOE approach to security has evolved since 9/11 from something that is akin to industrial security to a system involving an elite paramilitary force that can defend against a sophisticated terrorist attack. This has been a challenge both because of the need to enhance the capabilities of the protective forces and because the change has entailed significant expense to strengthen security structures and systems at facilities that were not initially designed with this type of security in mind. These changes had to be undertaken within budgetary limitations at a time when the Department needed to pursue many other important (and expensive) programs. The changing demands on the weapons complex over the years have added yet another layer of complexity. And any change in security had to be accomplished within a legal and administrative structure for the Department that is extraordinarily complicated.

The Department has not lacked for an abundance of thoughtful studies on the security issue over the years. Considerable change has been introduced as a result, but the Y-12 episode reveals that problems remain. Although my examination of the security issues confronting the Department has necessarily been limited, I am satisfied that the Y-12 episode has been taken very seriously and considerable effort has been made to ensure that security is strong throughout the complex. I have thus focused on your request to consider whether there are issues relating to the management structure for physical security. I know that you seek confidence that the security obligation will be fulfilled in an effective way for the long term.

You specifically asked whether the wholesale modification of the management structure for physical security is appropriate. As you know, the current system relies on contractors to provide security. (The details of this approach are discussed further below.) The obvious alternative would be to federalize the protective force (partially or completely) so that the security officers become DOE employees. Federalization could shorten chains of command between federal policymakers and the implementers of security, would encourage consistent application of policies and procedures across sites, would reflect the reality that security is a central federal function at these sites, and perhaps most importantly, would eliminate the potential for strikes by the protective force. Moreover, I understand that the unions at one time advocated such a change in order to deal with retirement and long-term disability concerns of the security officers.

An evaluation by DOE in 2009 concluded that the merits of federalization turned on three factors: implementation of elite force concepts in a cost-effective manner, determination of practical avenues to address retirement and disability concerns, and identification of methods to address potential protective force work stoppages. Memorandum to the Acting Deputy Secretary from T.P. D'Agostino and G.S. Podonsky (Jan. 13, 2009). The review found that the cost issue was the most important factor that should guide a decision and concluded that federalization would result in increased costs without commensurate benefits, particularly given the progress that had been made in implementing the elite force approach using contractors. The review also concluded that federalization did not offer a viable approach to address the union concerns because of the difficulties and complexities of a transition of guards from private-sector employment to federal employment. And, although it acknowledged that the most compelling reason to pursue federalization was to prevent work stoppages by unionized protective force members, it concluded that this risk could be managed by the execution of contingency protective force operations in such a situation, an approach that DOE has had to take in connection with a strike at Pantex. Although to my mind the issue is a close one, I have no informed basis to challenge this recent evaluation.

One additional factor in favor of federalization is that a dramatic change of this nature could facilitate the introduction of a new security culture. In a sense, such a step would serve to wipe the slate clean and demonstrate that very different performance is expected going forward. The Office of Secure Transport uses federal employees and has satisfactorily fulfilled its functions, which serves to show that federalization can work. But no doubt a wholesale change in management structure would be very expensive to accomplish. And, if the protective force were federal employees, the imposition of discipline would be more difficult and in the end federalization could reduce flexibility.

A variant is limited federalization. For example, one might federalize the armed component of the protective forces, while relying on a contractor for the remaining services. This presumably would reduce the cost of the transition

and would recognize the unique federal role of those who are authorized to use deadly force. Since federal employees cannot strike, this approach would facilitate the ability to respond to a work stoppage. But this approach would then complicate the chains of command within the protective forces. And it would make even more difficult the challenge of providing a career path for those in the armed component of the protective forces. (This issue is discussed below.)

I conclude that a decision to federalize all or a part of the protective force would be difficult, would be expensive to accomplish, and would create some new challenges. In the absence of compelling benefits, it is probably not warranted. But it is an approach that may be worthy of consideration if efforts to make the necessary changes cannot be accomplished by a less drastic approach.

A variant to the federalization of the protective force as DOE employees is to engage another federal agency, such as the Department of Defense or the Department of Homeland Security, to provide security. Engagement of another agency to provide security would serve to complicate chains of command and would likely create confusion as to who was in charge at the sites. The interfaces between the DOE and the management and operations ("M&O") contractors would become even more complicated and confusing. Even if DOE were to engage another agency to provide security, the Department would still be accountable for the security posture. And, although I have not pursued the point, I am doubtful that another agency would be willing take on the task. I conclude that such an approach is not suitable.

I thus conclude that it is reasonable to continue to rely on private contractors to provide security. I hasten to add, however, that there are opportunities to improve the management of security. Some of my suggestions follow:

1. Align authority and responsibility. At Y-12, there was a division of responsibility for physical protection between the contractor responsible for the protective officers and the M&O contractor responsible for the fences, various sensors and other equipment that are part of the physical protection system. The result was a fractured management structure. The interface between the contractors was clearly not functioning: their priorities were not aligned. Cameras in the affected area were out of service and had been for a considerable time and the system of detectors, which had recently been significantly upgraded, was plagued by frequent false alarms. This resulted in a situation in July in which the protective force did not appreciate that the alarms associated with the breach of the fences were "real" and the absence of functioning cameras did not enable the appropriate immediate surveillance of the situation. Although no doubt a system involving multiple contractors could be made to work, a simplified structure in which one contractor is

responsible for all elements of security would provide greater assurance that the security approach is integrated and that issues that otherwise would cross lines between contractors are addressed.

Although a compelling case can be made for assuring that all security functions are the responsibility of a single contractor, there is a subsidiary question whether security should be the subject of a separate contract from that with the M&O contractor. The advantage of separation is that the security responsibility could be allocated to an entity with strong skills in that one area, whereas the M&O contractor presumably must be selected based on a balancing of a variety of capabilities. But, again, separating the security function from the overall site responsibility will require a complicated interface between contractors, with opportunities for miscommunication and misalignment of priorities: security should be an integral part of site operations, not an add-on. Indeed, a single chain of command will be mandatory during a security event. As a result, the favored course, it seems to me, is to require the M&O contractor to fulfill the security function and to ensure, through proper controls, that it meets its responsibilities.

2. Improve federal oversight. It was apparent that the department's system of oversight did not detect and correct the security problems that the Y-12 incident revealed. The large number of false alarms was tolerated, raising questions about the acceptance testing, readiness, and maintenance of the ARGUS system. The cameras were not viewed as critical security equipment, with the result that a significant number were inappropriately allowed to remain out of service for an extended period. There were significant departures from expected procedures by the first responder, as well as significant communication deficiencies. The DOE oversight "system" was seemingly unaware of these problems and, in fact, the evaluations of the security at Y-12 had received consistently high marks in the period before the incident. The overall situation reveals significant failings in oversight by DOE. I appreciate that the approach to oversight does implicate broader issues within the Department as to the degree of freedom and flexibility that should be provided to its contractors.

   Part of the challenge in providing proper oversight may relate to the extraordinarily complicated administrative structure within DOE, with security responsibilities spread across several offices at headquarters and between headquarters and the DOE field offices. Indeed, we have had some difficulty in obtaining a clear organization chart that defines the structure for security oversight within DOE. I understand that issues associated with diffuse management are subject to study within the National Nuclear Security Administration ("NNSA") in an effort that is being led by Brigadier General Sandra Finan. A broader examination of DOE's internal management of security should be undertaken in order to

streamline and simplify the structure. The aim should be to establish clear authority and responsibility and to assure that the responsible staff has the right training and experience. Although I appreciate that different approaches to security may well be appropriate as a result of differing circumstances at the various DOE sites, I question whether different standards can be justified as a result of DOE's organizational structure. Efforts to achieve consistency and uniformity would be appropriate.

3. Enhancement of the Protective Force. Perhaps the most puzzling aspect of the Y-12 incident is the behavior of the first responder. He had evidently received the appropriate training, but decided to ignore it. He seems to have immediately concluded that the three intruders were not a threat and, as a result, he treated them as such. Although his assessment proved to be correct, attackers might seek cover for a serious assault by mimicking the appearances that evidently were so reassuring to the first responder. The episode reveals the importance of training and drills to reinforce appropriate actions by the protective force.

   There are challenges associated with the maintenance of an appropriately trained protective force. DOE has enhanced the capabilities of its protective forces significantly with the aim of a establishing an elite paramilitary capability that can respond to a very capable and sophisticated adversary. The physical qualifications and capabilities of many members of the force must be maintained at a high level, which creates a challenge in establishing a career trajectory for the protective officers. Having a force that maintains its "edge" is difficult, given that actual attacks have not occurred. Indeed, overcoming boredom among the members of the protective force is difficult. The commercial nuclear industry has confronted many of these same challenges and has sought to establish and maintain an esprit among the protective force. It encourages attentiveness by frequent force-on-force drills, regular transitions among posts, and allowing other activities, such as access to the web while on post, in appropriate circumstances. It has sought to respond to the demanding physical challenges that may become more difficult as the security officers age by enabling and encouraging them to migrate to other jobs at the site. In short, it has sought to establish and reinforce that the protective force is an important part of the team that operates the plant and that its members have career opportunities. Some of these lessons may be relevant to the DOE sites.

4. Security Culture. The commercial nuclear industry has learned that the essential ingredient for assuring safe operations is the establishment of a culture in which safety is the highest priority. Management has the obligation to establish such a culture by its words and deeds, including the allocation of resources. Each plant worker has an individual responsibility to assure that any safety issue that a worker observes is

addressed even it is not within the worker's responsibilities; if a supervisor fails to respond, the worker is obligated to raise the issue to a higher level and severe sanctions are imposed if any retaliation against such a worker occurs. Given the critical importance of security at the Category I sites, I believe that an analogous security culture needs to be established at the DOE sites. That is, everyone on the site should understand that security is his or her responsibility. Establishing such a culture will be difficult in a system in which individuals are otherwise encouraged to focus on individual responsibilities, but truly effective security requires such a change.

5. Balance. The Y-12 episode has appropriately caused a heightened awareness of the importance of physical security. This focus should not be allowed to unduly distort DOE's efforts. The aim should be to evaluate security using a systems approach that integrates physical, cyber, and personnel security in order to reduce aggregate vulnerabilities. Balance should be maintained.

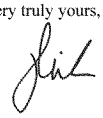
* * *

In developing my thinking on the charge that you presented, I have had the benefit of interactions with Norm Augustine and Don Alston, as well as substantial assistance from the Center for Strategic and International Studies ("CSIS"). I was aided by extensive materials assembled by CSIS with DOE assistance concerning the various security reviews undertaken over the years, by site visits, by discussions with DOE and contractor staff, and by interviews with knowledgeable individuals. (Some of these interviews were undertaken by CSIS staff.) I very much appreciate this assistance. Nonetheless, this letter reflects my perspective. My comments should not be attributed to the various individuals who have helped to shape my judgments.

I hope this letter is helpful. Please feel free to contact me if you have any questions.

Best regards.

Very truly yours,



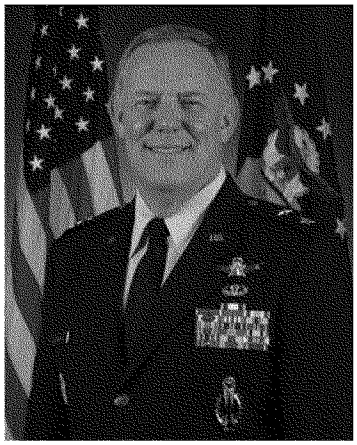
Richard A. Meserve

# BIOGRAPHY

**UNITED STATES AIR FORCE**

## MAJOR GENERAL C. DONALD ALSTON

**Retired Sep. 1, 2012.**



In his last assignment, Maj. Gen. C. Donald Alston was Commander, 20th Air Force, Air Force Global Strike Command, and Commander, Task Force 214, U.S. Strategic Command, Francis E. Warren Air Force Base, Wyo. He was responsible for the nation's intercontinental ballistic missile force, organized into three operational wings with more than 9,600 people.

General Alston was commissioned in 1978 following graduation from the U.S. Air Force Academy. He has commanded at the squadron, group and wing levels and served as the first Assistant Chief of Staff, Strategic Deterrence and Nuclear Integration at Headquarters U.S. Air Force. He has worked as a liaison officer to the U.S. House of Representatives, and also performed duties as the executive assistant to the Secretary of the Air Force in Washington, D.C. General Alston also served as the Deputy Chief of Staff for Strategic Communications and the spokesperson for Multi-National Force - Iraq in Baghdad.

**EDUCATION**

1978 Bachelor of Science degree, U.S. Air Force Academy, Colorado Springs, Colo.
1984 Squadron Officer School, Maxwell AFB, Ala.
1986 Air Command and Staff College, by correspondence
1986 Master's degree in business administration, Golden Gate University, Calif.
1995 Air War College, Maxwell AFB, Ala.
1998 Armed Forces Staff College, Norfolk, Va.
2003 National Security Management Course, Maxwell School of Citizenship and Public Affairs, Syracuse University
2011 Senior Executives in National and International Security Program, Harvard University, John F. Kennedy School of Government, Executive Education

**ASSIGNMENTS**

1. July 1978 - January 1979, ICBM combat crew training, Sheppard AFB, Texas; and Vandenberg AFB, Calif.
2. January 1979 - December 1980, deputy missile combat crew commander, 571st Strategic Missile

Squadron; and instructor and deputy missile combat crew member, 390th Strategic Missile Wing, Davis-Monthan AFB, Ariz.
3. January 1981 - February 1982, Titan II missile combat crew commander, 570th Strategic Missile Squadron, Davis-Monthan AFB, Ariz.
4. February 1982 - March 1984, emergency war order training instructor, 390th Strategic Missile Wing, Davis-Monthan AFB, Ariz.
5. March 1984 - May 1984, student, Squadron Officer School, Maxwell AFB, Ala.
6. May 1984 - August 1987, Chief, Emergency War Order Training Branch, and Chief, Plans Division, Directorate of Missiles, Headquarters 15th Air Force, March AFB, Calif.
7. August 1987 - December 1990, congressional inquiries officer, later, liaison officer, U.S. House of Representatives, Air Force Legislative Liaison, Office of the Secretary of the Air Force, Washington, D.C.
8. January 1991 - March 1993, executive assistant to the Secretary of the Air Force, Office of the Secretary of the Air Force, Washington, D.C.
9. June 1993 - July 1994, Commander, 12th Missile Squadron, Malmstrom AFB, Mont.
10. August 1994 - June 1995, student, Air War College, Maxwell AFB, Ala.
11. June 1995 - May 1996, Deputy Director, Commander's Action Group, Headquarters Air Force Space Command, Peterson AFB, Colo.
12. May 1996 - July 1997, executive officer to the Vice Commander, Headquarters Air Force Space Command, Peterson AFB, Colo.
13. July 1997 - July 1999, Chief, Requirements Integration Branch, later, Chief, Integration Division, Directorate of Plans, U.S. Space Command, Peterson AFB, Colo.
14. August 1999 - March 2001, Commander, 341st Operations Group, Malmstrom AFB, Mont.
15. March 2001 - July 2002, Vice Commander, 21st Space Wing, Peterson AFB, Colo.
16. July 2002 - July 2004, Commander, 341st Space Wing, Malmstrom AFB, Mont.
17. July 2004 - February 2005, Assistant Director, Air and Space Operations, Headquarters Air Force Space Command, Peterson AFB, Colo.
18. February 2005 - February 2006, Deputy Chief of Staff, Strategic Communications, and spokesperson, Multi-National Force - Iraq, Baghdad, Iraq
19. February 2006 - September 2007, Director of Air, Space and Information Operations, Headquarters Air Force Space Command, Peterson AFB, Colo.
20. September 2007 - February 2008, Director, Space and Nuclear Operations, Office of the Deputy Chief of Staff for Air, Space and Information Operations, Plans and Requirements, Headquarters U.S. Air Force, Washington, D.C.
21. February 2008 - October 2008, Director, Nuclear Operations, Plans and Requirements, Deputy Chief of Staff for Operations, Plans and Requirements, Headquarters U.S. Air Force, Washington, D.C.
22. November 2008 - June 2010, Assistant Chief of Staff, Strategic Deterrence and Nuclear Integration, Headquarters U.S. Air Force, Washington, D.C.
23. July 2010 - present, Commander, 20th Air Force, Air Force Global Strike Command, and Commander, Task Force 214, U.S. Strategic Command, Francis E. Warren AFB, Wyo.

**SUMMARY OF JOINT ASSIGNMENTS**
1. May 1997 - May 1998, Chief, Requirements and Integration Branch, Headquarters USSPACECOM, Peterson AFB, Colo., as a lieutenant colonel
2. May 1998 - May 1999, Chief, Integration Division, Headquarters USSPACECOM, Peterson AFB, Colo., as a colonel
3. February 2005 - February 2006, Chief, Communications Division, Strategic Effects, Multi-National Force - Iraq, Baghdad, Iraq, as a brigadier general

**OPERATIONAL INFORMATION**
Badges: Master Missile Badge with operations designator; Master Space Badge; basic parachutist
Weapon Systems: Titan II, Minuteman III A-M CDB, Minuteman III REACT A/B

**MAJOR AWARDS AND DECORATIONS**
Distinguished Service Medal
Legion of Merit with oak leaf cluster

Bronze Star Medal
Defense Meritorious Service Medal
Meritorious Service Medal with four oak leaf clusters
Joint Service Commendation Medal
Air Force Commendation Medal with oak leaf cluster
Air Force Achievement Medal with oak leaf cluster
Air Force Outstanding Unit Award with silver and three bronze oak leaf clusters
Air Force Organizational Excellence Award
Combat Readiness Medal
National Defense Service Medal with bronze star
Iraq Campaign Medal

**EFFECTIVE DATES OF PROMOTION**
Second Lieutenant May 31, 1978
First Lieutenant May 31, 1980
Captain May 31, 1982
Major April 1, 1989
Lieutenant Colonel June 1, 1993
Colonel Sept. 1, 1998
Brigadier General Aug. 1, 2005
Major General Sept. 2, 2008

(Current as of December 2011)

NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON STRATEGIC FORCES
UNITED STATES HOUSE OF REPRESENTATIVES

PRESENTATION TO THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON STRATEGIC FORCES
U.S. HOUSE OF REPRESENTATIVES

SUBJECT: Nuclear Security: Actions, Accountability, and Reform

STATEMENT OF: Brigadier General Sandra E. Finan
Commander, Air Force Nuclear Weapons Center
Based on Previous Position as
Acting Chief of Defense Nuclear Security, NNSA

February 28, 2013

NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON STRATEGIC FORCES
UNITED STATES HOUSE OF REPRESENTATIVES

**Introduction**

Chairman Rogers, Ranking Member Cooper, distinguished Members of the Committee, thank you for the opportunity to discuss the study I conducted on the National Nuclear Security Administration's (NNSA) federal security organization and assessment model. Although I am no longer assigned to the NNSA, I am pleased to share our observations based on our 90 day study.

In the aftermath of the July 28, 2012 security incident at the National Nuclear Security Administration's Y-12 National Security Complex, the leadership of the NNSA and the Department of Energy (DOE) took action to address the security failures at Y-12. The initial information gathered revealed that issues at Y-12 were part of a larger pattern of security program management deficiencies within the NNSA. These security issues prompted the NNSA Administrator to commission a Task Force to analyze the current Federal NNSA security organizational structure and security oversight model and recommend possible improvements. The NNSA Administrator directed the Task Force to:

- Analyze current NNSA security organizational structure and recommend possible improvements that would improve operational focus, oversight, and culture sustainment.
- Analyze current NNSA security oversight model and mechanisms to determine what seams exist and what structures could be implemented to better ensure that the issues are found and fixed before they become problems.

While other reviews were aimed at diagnosing the root causes of the Y-12 event, the NNSA Administrator's direction called for this Task Force to focus on the "path forward" within the Federal NNSA organization. Under my leadership, the Task Force consisting of NNSA, DOE,

and military specialists conducted extensive document reviews and interviewed Federal managers and staff as well as a selection of contractor security managers and others across the NNSA security organization. The Task Force collected and analyzed information, identified issues, and suggested a revised organizational structure and assessment model.

While we highlighted negative aspects of the NNSA security organization and assessment model, the Task Force found many great people on the NNSA security staffs. They are clearly dedicated, skilled, and hard-working and want to get the security mission done right. Unfortunately, NNSA security personnel have seen themselves thwarted by lack of management support and feel obstructed by some of their peers. Their difficulties were compounded by the absence of a workforce strategy to recruit, retain, and develop a cadre of talented, knowledgeable and experienced security professionals. Thus, it is all the more encouraging that these personnel, almost without exception, genuinely care about doing good work. Their continued strong desire to build a successful security organization is a hopeful sign for the future.

**Summary Findings**

The Task Force noted significant deficiencies in security organization, oversight, and culture sustainment throughout the NNSA security organizations. In the NNSA security organizations, line management authority was ill-defined and claimed by multiple Federal NNSA organizations. On the one hand, the "Federal field organizations" (federal site offices and the nuclear production office which oversees the management and operating contracts) exercised line management authority over the site security contractors via the contract management structure. On the other hand, the NNSA Headquarters security organization asserted that it also had such authority. Absent clearly defined lines of authority, many individuals asserted authority, while correspondingly few have assigned responsibility. This lack of clear lines of authority

contributed to a widespread practice of decision-making by consensus. When consensus failed, organizational elements acted independently or not at all, which undermined effective implementation of the security program.

The Task Force further noted a significant gap in the current NNSA security organizational structure. At the strategic level the NNSA Headquarters organization had been ineffective and had intervened in field tactical execution. The Federal field organizations had been ineffective in performing their tactical responsibilities for executing the security program and had intervened in strategic matters. Additionally, there had not been a clearly identified operationally-focused organization that bridged the gap between strategic and tactical responsibilities and addressed standardization, field execution, and multi-site analysis.

The Task Force found a weak security performance assessment model. It found that NNSA relied overwhelmingly upon Federal staff simply reviewing contractor-provided data, rather than effectively assessing performance itself. At the same time, misinterpretation of the DOE Safety and Security Reform Plan resulted in less stringent independent oversight of security operations. As a result of numerous interviews, the Task Force also observed that potentially critical management information was not being reported clearly to the appropriate decision makers.

As concerning as these structural and assessment issues might be, the most striking result of this review falls in the area of culture sustainment. It quickly became evident that the Task Force findings closely resembled those presented in numerous prior reports. While NNSA has attempted to correct some identified issues over the years, it has not adequately emphasized effective security mission performance. In recent years, NNSA security leaders have chosen to emphasize security cost containment to the detriment of security program execution. The idea that the requirements for security performance effectiveness are subordinated to cost concerns

had become a prevailing concept in the NNSA security community. This emphasis had become endemic throughout the NNSA security culture, so much so that fundamental facility protection issues such as the protection of operational capabilities came to be regarded as too expensive and therefore "out of bounds" for analysis. The NNSA security culture had focused on fiscal limitations over effective performance. This resulted in an environment in which deficiencies were worked at the margins rather than management addressing core issues.

These issues underscored the critical role of effective leaders. While outside the charter of this Task Force, it must be acknowledged that leadership plays the key role in mission accomplishment. The Task Force recognized that effective leadership may compensate for structural deficiencies within an organization; however, restructuring alone cannot overcome leadership shortcomings. The best assessment model is useless if leaders fail to effectively implement it. Additionally, the assessment model will not be effective unless leaders consistently demand comprehensive, unbiased information. NNSA must take ownership of its history of security failures. Leadership must take bold and enduring actions if this pattern is to be broken.

**NNSA Organizational Model**

The existing NNSA security organizational structure was convoluted and ineffective. The Task Force observed that lines of authority in virtually every organizational function were divided. The NNSA security function was not well organized or effectively staffed and the NA-70 policy development and implementation process was sub-standard. While the Chief of Defense Nuclear Security is the Cognizant Security Authority (CSA), this responsibility has been unevenly delegated and was open to inconsistent interpretation. Security staffs were responsible to multiple lines of authority and for some functions may not be responsible to anyone. The most

fundamental issues arose from the relationship between NA-70 and the Federal field organizations. NA-70 believed that it had line management authority over the security elements within the Federal field organizations. However, the managers of these field organizations had been formally assigned line management authority. The NNSA Act states that the Chief of Defense Nuclear Security role includes "the development and implementation of security programs". The current interpretation of this provision has been a source of ambiguity due to the mixing of line and staff responsibilities.

**Roles and responsibilities were either undefined or not followed.** The Task Force identified numerous occasions across the NNSA security organizations where individuals were not allowed to perform assigned duties or assumed roles and responsibilities nominally assigned to others. The confusion of roles and responsibilities was evident in NA-70, within field organizations, and between NA-70 and the field. For example, the approved mission and function statements for the two major divisions within NA-70 have little apparent relationship to the way these offices operated and how they interacted with each other or with the NA-70. Within field organizations, the Task Force noted a number of instances where management precluded staff from performing the assigned roles of their position and/or assigned personnel to unrelated duties. At times, NA-70 acted as a formal line management organization, and asserted responsibilities that were formally assigned to the Federal field security organizations. NA-70 personnel were frequently frustrated by site-level resistance to the programmatic direction they provided and Federal field security managers were often similarly frustrated when NA-70 used its budget authority, its control over the policy process, and other activities to inject itself into what the sites regard as their line management decision-making process.

**There were no clear lines of authority.** There were overlapping lines of authority and mixed staff and line functions. The CSA function flowed from the NNSA Administrator through the Chief of Defense Nuclear Security to the Federal field organizations. Line management authority went from the NNSA Administrator through the Associate Administrator for Infrastructure and Operations (NA- 00), to the field. However, NA-70 attempted to exert line management authority and provided programmatic guidance directly to the Federal field security managers. While Federal field organizations administer the contracts governing the actual performance of the security mission, NA-70 routinely interacted with the security contractors. Furthermore, NA-70, not the line managers, was the primary executer of the NNSA security budget.

**The security policy process was sub-standard.** The Task Force identified that there was no clearly articulated or consistently implemented NNSA security policy process. A major concern was the supplanting of DOE Security Orders with generic and less restrictive NNSA policies (NAPs). This appeared to be based on a desire to reduce funding demands through a reduction of requirements. Additionally, the Task Force noted a desire on the part of some NA-70 senior managers to maximize separation from DOE HSS policies and activities. Within NA-70, policy and guidance were issued through a variety of formal and informal mechanisms with erratic distribution. The Task Force identified that some Federal field organizations were inconsistent in their acceptance and application of NA-70 issued policies. Finally, NA-70 policy and guidance tended to be vague resulting in widely differing interpretations by field personnel.

**The NNSA Federal security organization was not effectively structured or staffed.** While there were clearly strategic (Headquarters) and tactical (Federal field organizations and contractors) levels, there was little indication of an effective operational element with

responsibility for security program functions such as site assistance and standardization of program execution. The Task Force also noted that the Federal field organizations structured their security functions substantially differently. This resulted in a lack of standardization of both organization and execution of the security program. At some sites there was weakening of the security function and reduced senior management attention. There were a number of personnel issues associated with the security professional staff including the lack of a human capital development plan, no career path, and limited mobility. Additionally, the Task Force noted an overreliance on support service contractors who primarily assisted the NA-70 organization.

**Federal Assessment Model**

The Task Force expended considerable effort attempting to describe, understand and analyze the current assessment model and mechanisms.

The failure to adequately assess security system performance and to clearly and unequivocally report deficiencies to the appropriate senior managers has been identified as a significant contributing cause to the Y-12 security incident. The Task Force focused upon the performance assessment process as implemented by Federal field and Headquarters organizations within NNSA. Although contractor self-assessments were the first-line elements in the security performance assessment process, these were outside the direct scope of the review. Strengthening the contractor self-assessment process is an important objective, but cannot replace a rigorous Federal assessment process.

**NNSA did not have an adequate security performance assessment process or capability.** The performance assessment capabilities of Federal security organizations within NNSA were

virtually non-existent. Essentially all responsibility for performance assessment was delegated to the Federal field organizations. The current Federal field organizations were typically limited to "shadowing" contractor self-assessments and/or reviewing the reports these self-assessments generated. Moreover, there was a tendency on the part of some field Federal staff to adopt the role of defending "their" contractors rather than attempting to objectively assess contractor performance. At the Headquarters level, the NA-70 performance assessment function had only three full-time Federal staff members. The Task Force noted that the NA-70 assessment process was largely confined to the review of submitted paperwork. The result was that there was no NNSA Federal organization capable of performing effective security performance assessment.

**The "systems-based" assessment model as implemented was ineffective for security.** Misinterpretation, and/or misapplication of the DOE Safety and Security Reform Plan, dated March 16, 2010, resulted in a weakened Federal security assessment program. In particular, this document stated: "Security Performance: Contractors are provided the flexibility to tailor and implement security programs in light of their situation and to develop corresponding risk- and performance-based protection strategies without excessive Federal oversight or overly-prescriptive Departmental requirements." This guidance was further expanded upon and eventually articulated in NAP-21, Transformation Governance and Oversight Initiative. The belief arose that 'eyes on, hands off' precluded Federal security staff from conducting performance-based assessments of contractors. As a result, most Federal assessment was based on paperwork generated by the contractor. This paper-based system of assessment, without sufficient performance verification, was inadequate for effective evaluation of security operations.

**NNSA had no clear and consistent performance baseline for security program implementation.** A performance baseline, set forth in detailed standards and criteria, is the keystone of an effective security program. Precisely articulated standards and criteria further provide an objective foundation for performance assessment. NNSA did not have the standards or criteria necessary to effectively measure security program performance. The absence of such standards and criteria diminished the ability to identify potentially significant performance deficiencies. The Task Force noted that the lack of standards and criteria had been coupled with the widespread notion that contractors must only be told "what" the mission is, not "how" the mission is to be accomplished. While this approach may be appropriate in other areas, it was ineffective as applied to security programs. Therefore, security tasks were not necessarily performed in a manner consistent with NNSA security requirements.

**The current assessment process was biased against criticism.** The Task Force noted a distinct bias against finding and stating performance criticisms. The NNSA Federal assessment relies heavily on contractor self-assessment. While an important and useful tool, contractor self-assessments tend to be insufficiently objective. The primary Federal assessment role was performed by field staff. Long-term geographic proximity to site contractors can compromise the objectivity of these Federal assessors. Moreover, the intermingling of management and assessment roles within Federal field organizations can also contribute to less objective assessment. The NA-70 Headquarters performance assessment process, being paper-based, could not validate the information submitted. Information provided to the Task Force suggested that in some instances information considered to be unfavorable was being "watered down" or obscured. Furthermore, information was presented that indicate differing opinions were being

suppressed by some senior managers in the field and at Headquarters. As a result, NNSA senior leadership may not have received all information needed to make quality decisions.

**Recommended Organizational Structure**

Recommend an organizational structure that separates the line function for executing the security mission from the Headquarters staff function. Additionally, create an operational-level organization that focuses on security implementation and standardization. Distinct roles and responsibilities should be associated with tactical, operational, and strategic-level security functions. Tactical execution of contract administration occurs at the Federal field organizations. Operational implementation and standardization of operations across the security program occurs at the NA-00 level. Strategic-level policy guidance, requirements determination, and performance assessment occur in Headquarters NNSA, NA-70.

In order to clarify the line of authority, CSA must flow from the NNSA Administrator, through the head of the NA-00, to the Federal field managers, and finally to the designated CSA at field sites, with no re-delegations authorized to non-Federal individuals. This authority should follow the same path as the line authority. The asserted security line management tie between the Chief of Defense Nuclear Security and the security managers in the field should be terminated in order to ensure a single, clear line of authority.

In terms of clarifying line and staff functions, the current NA-70 organization needs to be restructured so that it serves solely as a staff organization at the strategic level. Specific alignment within the divisions can be varied. The most important change in NA-70 is the stand-up of the Performance Assessment Division -- a new function responsible for assessment of

contractor and Federal field organization performance. This is the entity that the Chief of Defense Nuclear Security would use to verify that security programs are properly implemented.

A new security operations organizational level needs to be stood up within the NA-00 structure. The responsibilities of this office are to ensure that the policies and guidance provided by the NA-70 staff are executed in the field. It will also ensure standardization of security procedures across the field locations as well as provide field assistance, and a conduit for field concerns to be surfaced to the NA-70 staff.

Resource planning and budgeting, and project management responsibilities will be realigned from NA-70 to the new operational-level organization. This establishes a clear linkage between budget formulation and mission execution and establishes an equally clear boundary between budget considerations and the formulation of requirements. An expanded intelligence/counterintelligence liaison is intended to ensure that Federal security managers get needed information and have appropriate ties to law enforcement and intelligence-related agencies.

At the tactical level in the field, the multiple lines of authority are eliminated and direction will come from a single line of authority. All authorities will run through the Federal field organization manager to the appropriate security manager. The Federal field organization scope of duties will include primary contract administrative functions--including reviews of contractor reports, analysis, security plans, and other required documentation; partnering with the executing contractor; remaining knowledgeable and up-to-date on the content, operations, and effectiveness of the contractor's security implementation; alerting management of all concerns related to contractor execution of the security mission.

This organizational structure will help define and clarify roles and responsibilities and facilitate a strong mission focus. It divides resourcing from requirements determination in order to ensure that requirements are appropriately stated, weighed against budget resources and decisions made on accepting risks at the appropriate level. It provides a single line of authority to those operating in the field and maintains an appropriate span of control.

**Recommended Assessment Model**

Recommend a three-tiered assessment process that strengthens the role of Federal security assessment within NNSA without diminishing the legitimate need for contractors to maintain their own self-assessment capabilities.

The contractor self-assessment process continues as a first tier in the overall assessment process. The primary audience for the contractor self-assessments should be the contractor security managers themselves. However, the self-assessments should follow a consistent, program-wide format, and be made available for review at all higher levels of management. Contractors should be required to identify, report, and resolve security issues--sanctions should come when a higher level assessment uncovers problems that the contractor self-assessments fail to identify or properly address. Even when an issue is readily resolved and corrective actions are immediate, a finding should be issued and the corrective action recorded. Failure to do so inevitably hides potential negative trends. Contractor self-assessments should involve active performance testing rather than simply relying on work observation and document review--effective security performance can only be evaluated through testing.

The fundamental purpose of Federal security performance assessment is to ensure that requirements are properly implemented. Therefore, the primary Federal assessment organization

should ultimately report to the Chief of Defense Nuclear Security, who is responsible for requirements. This provides independence not only from the contractors, but also from the tactical-level Federal field staff whose necessary day-to-day interaction with contractor managers and staff risks loss of objectivity. This enables the Chief of Defense Nuclear Security to better ensure effective implementation of NNSA security programs. Additionally, it provides feedback on performance to the operational and tactical levels.

These Federal security assessments should include performance testing of all critical elements. The assessors should issue clear findings which are to be tracked and closed in a program-wide corrective action management system. Federal assessors should also look closely at the contractor self-assessment process; "failures to identify" by the contractor self-assessment element should automatically rise to the level of significant findings.

The final tier of the assessment model should explicitly rely upon the services of the independent security oversight function currently provided by HSS. NNSA should arrange for a regular process of comprehensive inspections. The oversight function should be encouraged to issue strong findings for matters of potential concern to the NNSA Administrator and the Secretary of Energy, and should routinely evaluate the performance of contractor self-assessments and the Federal assessment program.

This performance assessment model assumes a common requirements base that is employed at all levels and across the NNSA security program. While some allowance may be made for site-specific issues, the fundamental elements of this requirements base should be an appropriately integrated system of DOE policies, NNSA implementation directives, and field operational guidance. The requirements base should be reflected in approved documents such as site Safeguards and Security Plans. Specific performance requirements should be articulated in

detailed performance standards and criteria supported by a commonly understood and utilized performance testing process.

**Closing**

Over the years, there has been tension between implementation of security and conduct of operations. Whenever there have been significant incidents of security concern, there have been corresponding swings of the pendulum towards a more rigorous security program. Security program emphasis has increased after espionage cases, internal security lapses, and external events such as the September 11, 2001 attacks. However, over time, the general trend has been to accept more risk and to reduce the perceived burden and cost of the security mission. Furthermore, the trend has been to remove security from an integral mission role, adversely affecting the NNSA security program. The events at Y-12 illustrate how far the pendulum has swung in the wrong direction.

The Secretary of Energy characterized the Y-12 events as "unacceptable" and clearly stated that security is the highest organizational priority. The NNSA Administrator has been equally emphatic in numerous public statements since the incident. The evidence from Y-12 and from prior security incidents points to a culture of compromises. Moving forward, NNSA must establish and sustain an effective security program. NNSA must address the significant flaws in the current organizational structure for security and the associated assessment model. NNSA must clearly and consistently emphasize the importance of security. Ensuring that the right leadership is in the right position is absolutely critical to success. The daunting prospect—and the one that will require the consistent emphasis of current and future Secretaries of Energy and future Administrators of the NNSA—will be to instill a culture that embraces security as a

fundamental and essential element of the NNSA mission. If NNSA fails in this, then senior leaders will again find themselves answering to the American people for the failures of security. Sooner or later, the perpetrator will not be peacefully-minded.

# BIOGRAPHY

UNITED STATES AIR FORCE

## BRIGADIER GENERAL SANDRA E. FINAN



Brig. Gen. Sandra E. Finan is the Commander, Air Force Nuclear Weapons Center, Kirtland Air Force Base, N.M. The center is composed of a headquarters staff, one wing and two wing-equivalent directorates: the 377th Air Base Wing and Nuclear Capabilities Directorate at Kirtland AFB; and the ICBM Systems Directorate at Hill AFB, Utah. The AFNWC comprises more than 3,500 Airmen at 11 locations in the United States and Europe and is responsible for the entire scope of nuclear weapons sustainment functions.

General Finan entered the Air National Guard in 1982 as an enlisted cryptographic equipment repairperson. She received her Air Force commission in 1985 as a distinguished graduate of Officer Training School. She has served in a variety of space and nuclear assignments in missile crew operations; training and evaluations; satellite command and control; and satellite operations. The general has held senior staff assignments as the Air Force Global Strike Command Inspector General and the Air Force Space Command Director of Nuclear Operations.

Her commands include a space operations squadron and missile wing. General Finan has deployed to the Combined Air Operations Center in Southwest Asia as the Director of Space Forces in support of Operations Iraqi Freedom and Enduring Freedom. Previously, she was the Principal Assistant Deputy Administrator for Military Application, Office of Defense Programs, National Nuclear Security Administration, Department of Energy.

**EDUCATION**

1978 Bachelor of Arts in music education, California State University, San Bernardino
1989 Squadron Officer School, Maxwell AFB, Ala.
1989 Master of Science in systems management, University of Southern California, Los Angeles
1997 Master of Arts in national defense and strategic studies, Naval Command and Staff College, Newport, R.I.
1997 Armed Forces Staff College, Norfolk, Va.
2004 Master of Strategic Studies degree, Air War College, Maxwell AFB, Ala.
2006 National Security Fellow, Syracuse University, N.Y.

**ASSIGNMENTS**

1. November 1982 - January 1985, Air National Guard cryptographic technician and Air Force Reserve military training instructor, Lackland AFB, Texas
2. April 1985 - May 1987, protocol officer and executive officer, 2nd Bombardment Wing, Barksdale AFB, La.
3. June 1987 - August 1987, student, undergraduate missile training, Vandenberg AFB, Calif.

4. September 1987 - August 1991, senior evaluator commander and missile combat crew member, 341st Missile Wing, Malmstrom AFB, Mont.
5. September 1991 - September 1993, command operations evaluator, 3901st Missile Evaluation Squadron, Vandenberg AFB, Calif.
6. October 1993 - June 1996, program manager; Chief, Standardization and Evaluation; and chief, Training Programs, 20th Air Force, F.E. Warren AFB, Wyo.
7. July 1996 - June 1997, student, Naval Command and Staff College, Newport, R.I.
8. July 1997 - September 1997, student, Joint Professional Military Education Phase II, Armed Forces Staff College, Norfolk, Va.
9. October 1997 - August 1999, special assistant to the Commander; executive assistant to the deputy commander; and National Military Command System command and control officer, U.S. Strategic Command, Offutt AFB, Neb.
10. September 1999 - August 2000, executive assistant to the Director of Security and Emergency Operations, Department of Energy, Washington, D.C.
11. September 2000 - June 2001, operations officer, 21st Space Operation Squadron, Onizuka Air Force Station, Calif.
12. July 2001 - June 2003, Commander, 21st Space Operations Squadron, and installation commander, Onizuka AFS, Calif.
13. July 2003 - May 2004, student, Air War College, Maxwell AFB, Ala.
14. June 2004 - July 2006, Vice Commander, 91st Missile Wing, Minot AFB, N.D.
15. July 2006 - May 2008, Commander, 341st Missile Wing, Malmstrom AFB, Mont.
16. June 2008 - August 2009, Director, Nuclear Operations, Headquarters Air Force Space Command, Peterson AFB, Colo.
17. September 2009 - December 2010, Inspector General, Headquarters Air Force Global Strike Command, Barksdale AFB, La.
18. January 2011 - January 2013, Principal Assistant Deputy Administrator for Military Application, Office of Defense Programs, National Nuclear Security Administration, Department of Energy, Washington, D.C.
19. February 2013 - present, Commander, Air Force Nuclear Weapons Center, Kirtland AFB, N.M.

**SUMMARY OF JOINT ASSIGNMENTS**
1. October 1997 - August 1999, special assistant to the Commander; executive assistant to the Deputy Commander; and National Military Command System command and control officer, U.S. Strategic Command, Offutt AFB, Neb., as a major and lieutenant colonel
2. September 1999 - August 2000, executive assistant to the Director of Security and Emergency Operations, Department of Energy, Washington, D.C., as a lieutenant colonel
3. January 2011 - January 2013, Principal Assistant Deputy Administrator for Military Application, Office of Defense Programs, National Nuclear Security Administration, Department of Energy, Washington, D.C., as a brigadier general

**BADGES**
Command Missile Badge with Operations Designator
Command Space Badge

**WEAPONS SYSTEMS**
Minuteman II ICBM Improved Launch Control System
Minuteman III Rapid Execution and Combat Target System
Inertial Upper Stage Booster
Air Force Satellite Control Network

**MAJOR AWARDS AND DECORATIONS**
Defense Superior Service Medal
Legion of Merit with two oak leaf clusters
Defense Meritorious Service Medal
Meritorious Service Medal with two oak leaf clusters
Joint Service Commendation Medal
Air Force Commendation Medal with oak leaf cluster
Air Force Achievement Medal with oak leaf cluster

Combat Readiness Medal

**EFFECTIVE DATES OF PROMOTION**
Second Lieutenant April 5, 1985
First Lieutenant April 5, 1987
Captain April 5, 1989
Major Aug. 1, 1996
Lieutenant Colonel July 1, 1999
Colonel Aug. 1, 2003
Brigadier General May 7, 2010

(Current as of February 2013)

Statement of Gregory H. Friedman

Inspector General

U.S. Department of Energy

Before the

Subcommittee on Strategic Forces

Committee on Armed Services

U.S. House of Representatives

"Nuclear Security: Actions, Accountability, and Reform"

FOR RELEASE ON DELIVERY
10:30 AM
February 28, 2013

Mr. Chairman and Members of the Subcommittee, I am pleased to be here at your request to testify on actions of the Office of Inspector General relating to the July 2012 security breach at the National Nuclear Security Administration's (NNSA) Y-12 National Security Complex (Y-12). I will also discuss related aspects of our work concerning contractor governance and physical security at Department of Energy and NNSA facilities.

NNSA was established under the National Defense Authorization Act of 2000 as a separately organized agency within the Department of Energy. This action was intended to allow NNSA to concentrate on its defense-related mission, free from other distractions. Its creation was, in large measure, a reaction to highly publicized concerns about management of the weapons complex. With an annual budget of nearly $12 billion, NNSA is charged with critically important national security missions relating to nuclear weapons refurbishment and storage, nuclear non-proliferation, and science and technology research.

Y-12 is one of four production facilities in NNSA's Nuclear Security Enterprise. The site focuses on the processing and storage of uranium, an activity essential to the safety, security and effectiveness of the U.S. nuclear weapons stockpile. Y-12 maintains a sophisticated security mechanism that relies on a well-trained and extensively-equipped Protective Force, advanced technology, and a variety of physical fortifications.

Y-12 had long enjoyed a reputation as one of the most secure facilities in the United States. That reputation was materially damaged in the early morning hours of July 28, 2012, when three

individuals gained access to the area surrounding the Highly Enriched Uranium Materials Facility at Y-12 and defaced the building. The security in place did not prevent this intrusion.

**Office of Inspector General Activities**

Response to Security Breach

In response to the security breach, Special Agents of the Office of Inspector General promptly effectuated the arrest of the alleged trespassers. We are currently working with the Department of Justice and the local U.S. Attorney's Office on this matter. Separately, we initiated an expedited review of the circumstances surrounding the security breach and on August 29, 2012, issued a report on the incident. This was the subject of a hearing before the Subcommittee on Oversight and Investigations, House of Representatives Committee on Energy and Commerce on September 12, 2012.

Our review identified multiple system failures on several levels.[1] We found troubling breakdowns involving:

- Inadequate response to alarms;
- Failures to maintain critical security equipment;
- Over-reliance on compensatory measures;
- Misunderstanding of security protocols;
- Poor communications; and,
- Weaknesses in contract and resource management.

[1]*Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex,* DOE/IG-0868, available at: http://energy.gov/sites/prod/files/IG-0868_0.pdf.

These issues directly contributed to an atmosphere in which trespassers were able to gain access to the protected security area directly adjacent to one of the Nation's most critically important and highly secured weapons-related facilities.

Especially important in light of the purpose of today's hearing, we found that the contractor governance system and Federal oversight failed to identify and correct early indicators of the breakdowns in security systems. These same issues also contributed to a compromise of test materials that were intended to be used in a follow-on comprehensive inspection of the Y-12 security posture.

Compromise of Test Materials

Subsequent to issuing our report on the Y-12 security breach, we received allegations that materials intended to be used by the Department of Energy's Office of Health, Safety and Security (HSS) to test Y-12 Protective Force personnel security knowledge had been compromised.[2] We immediately initiated a review to examine the allegations. We found that HSS performed a comprehensive inspection of the site's security organization following the July 28, 2012, security breach at Y-12. That inspection, initiated on August 27, 2012, included both practical exercises and tests designed to evaluate the knowledge, skills and abilities of the site's Protective Force.

On the night of August 29, 2012, an HSS inspector discovered a copy of a security knowledge test in a Protective Force patrol vehicle while conducting performance testing. This discovery

[2]*Review of the Compromise of Security Test Materials at the Y-12 National Security Complex,* DOE/IG-0875, available at: http://energy.gov/sites/prod/files/IG-0875_2.pdf.

led to concerns that the test had been improperly distributed to Protective Force personnel prior to its administration and that there appeared to be a compromise of the upcoming test.

Our inquiry confirmed that the security knowledge test, including answers to the test questions, was compromised and improperly distributed to the very individuals whose knowledge was to have been evaluated. Contractor Protective Force personnel testified uniformly that there was no intent to cheat on the HSS inspection. While we had no direct evidence to the contrary, we found the credibility of this testimony to be questionable, especially in light of test handling and distribution activities that, at best, demonstrated a lack of due care and negligence. The failure to properly safeguard the test prior to its administration was, in our opinion, inexplicable and inexcusable, especially given the intense focus on Y-12 and the security concerns at the site.

As with the Y-12 security intrusion itself, we noted that the level of Federal involvement in the NNSA's contractor governance system was, at the very least, not sufficient for preventing the compromise of the test material. In particular, we observed that a cognizant Federal security official failed to take an active role in reviewing or controlling the test because he did not believe it was his role to do so. He also claimed that he lacked sufficient knowledge of existing local security protocols to provide comments on the structure of the test. This lack of Federal involvement paralleled the contractor governance issues that we observed during our review of the Y-12 security intrusion.

In our view, responsible Federal officials should have the requisite knowledge to review and comment on Protective Force testing materials. Leaving it to the contractors to review a draft of the test, as was done in this case, is not an optimal situation.

Contractor Governance

The Y-12 security intrusion and test compromise issues raised serious concerns about NNSA's implementation of its contractor governance approach. NNSA's approach relies on contractors to assess and evaluate their own performance, with Federal oversight of contractor activities, especially with regard to nuclear safety and security. Since July 2007, the Department of Energy and NNSA have required contractors to implement self-assessment systems to measure performance and help ensure effective and efficient mission accomplishment. Given the near total reliance on contractor support for mission execution and, consequently, the importance of contractor performance, transparency and effectiveness efforts, we reviewed the development of contractor assurance systems by NNSA and its contractors.

We recently reported that, despite at least 5 years of effort, NNSA and its support offices and site contractors had not yet implemented fully functional and effective contractor assurance systems.[3] Specifically:

- The contractor governance system was rendered ineffective by what Federal site level officials referred to as an "eyes on, hands off" approach to contract management;
- Contractor weaknesses were not effectively communicated to senior management officials;

[3] *National Nuclear Security Administration Contractor Governance,* DOE/IG-0881, available at: http://energy.gov/sites/prod/files/IG-0881.pdf.

- Contractor self-assessments were not effective in identifying weaknesses; and,
- Performance metrics tracked in the assurance systems were not clearly linked to those contained in the contractor performance evaluation plans used to determine fees.

We found that NNSA had placed substantial reliance on its contractors' ability to self identify and correct weaknesses that threaten the safe, secure, effective and efficient operation of the Department's national security facilities. Our findings suggest that this reliance may be unjustified absent more intense Federal validation of contractor assertions.

To its credit, NNSA had identified deficiencies with contractor assurance system implementation and recognized the need to improve contractor assurance systems and its overall approach to contractor governance. In December 2012, an NNSA official told us that the agency has decided to overhaul its governance process. NNSA's planned initiative is an important step forward. Based on our body of work in NNSA, we believe that comprehensive and sustained effort in this area is critical.

Management Challenges

The specific issues of contractor governance and physical security may reflect broader issues facing the Department. Specifically, for over a decade, the Office of Inspector General has identified contract administration as a major Department of Energy management challenge. Because virtually all physical security at Departmental sites is contractor-provided, the way in which these contracts are administered and their enormous costs have been and continue to be major issues. To put this in perspective, we have reported that the Department spends more than

$1 billion per year protecting its facilities, related materials and data. Of this amount, nearly $700 million per year is spent on a complex-wide Protective Force staff of nearly 4,000 contractor professionals.

The Protective Force staff services are procured using three distinctly different primary mechanisms. At some facilities, the facility management contract includes a provision for Protective Force services as part of its prime contract. At other locations, the Protective Force is procured through a stand-alone prime contract awarded by the Department. Under the third model, the Protective Force is procured through a subcontract to the prime facility management contractor. These arrangements, which lack uniformity and consistency, result in at least 25 separate contract instruments.

In 2011, in our annual Management Challenges report, we concluded that there may be significant economy of scale cost benefits associated with Protective Force contract consolidation.[4] We proposed several alternatives, including the possibility of federalizing the Protective Force staff. We found that by either consolidating the contractor Protective Force or federalizing it, the Department could benefit from a more consistent approach to Protective Force organization, management, training, and equipment purchases. It could also improve the system for sharing security best practices and lessons learned between Department facilities, and providing the staff with greater career opportunities for advancement by allowing them to move between sites on a merit basis. Finally, consolidation itself would reduce the number of

[4] *Management Challenges at the Department of Energy – Fiscal Year 2012,* DOE/IG-0858, available at: http://energy.gov/sites/prod/files/IG-0858.pdf

contracts, minimizing administrative costs and simplifying the process of contractor accountability.

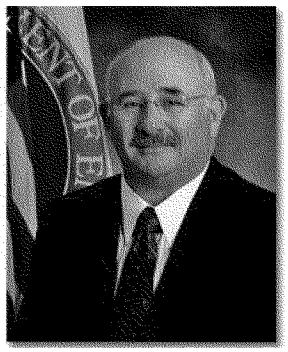
To its credit, NNSA has taken some action to consolidate the protective services at Y-12 and the Pantex Plant through its contract for the management of the sites. Specifically, the recently announced contract for consolidated management of the two sites includes Protective Force services to be provided by the new contractor.

**Observations**

The work of the Department of Energy and NNSA are essential to U.S. national security. While there is no quick fix or panacea to address the problems that are the topic of this hearing, we believe more enlightened, effective Federal oversight is necessary if progress is to be achieved.

This concludes my testimony and I look forward to your questions.

## GREGORY H. FRIEDMAN – DOE INSPECTOR GENERAL



Gregory H. Friedman was nominated by the President and confirmed by the U.S. Senate as Inspector General of the U.S. Department of Energy in 1998. Mr. Friedman started his Federal career in 1968 and has been with the Department of Energy, Office of Inspector General, since 1982. As Inspector General, he is responsible for a nationwide, independent program of audits, inspections, and law enforcement efforts related to the Department of Energy's programs and operations. In addition to his responsibilities as Inspector General, Mr. Friedman now serves as a member of the Recovery Act Accountability and Transparency Board and the Government Accountability and Transparency Board.

Mr. Friedman received a Bachelor's degree in Business Administration from Temple University and a Master's degree in Business Administration from Fairleigh Dickinson University. In 1979-1980, Mr. Friedman was selected as a Princeton Fellow in Public Affairs and spent a year in residence at Princeton University's Woodrow Wilson School for Public and International Studies.

In 2002, Mr. Friedman was named by the Comptroller General of the United States to serve as a member of the Advisory Council on Government Auditing Standards. In addition, he led the development of the "Federal Audit Manual," for the first time providing universal guidelines for conducting Federal financial audits.

From 2005 to 2008, Mr. Friedman served as Vice Chair of the President's Council on Integrity and Efficiency. Mr. Friedman has been a guest lecturer on the topics of audit, integrity, government oversight and program evaluation. In addition, Mr. Friedman is a member of several professional organizations, and has served in leadership positions in the Association of Government Accountants and the Institute of Internal Auditors. Mr. Friedman has also been active in a number of community and philanthropic organizations.

During his Federal career, Mr. Friedman has received numerous awards, including the Department of Energy's Meritorious Service Award, the Meritorious Presidential Rank Award, and the Presidential Rank Award for Distinguished Executive.

**Statement of**
**Hon. Daniel B. Poneman**
**Deputy Secretary**
**U.S. Department of Energy**

**Before the**
**Subcommittee on Strategic Forces**
**Committee on Armed Services**
**U.S. House of Representatives**

**February 28, 2013**

Chairman Rogers, Ranking Member Cooper, and members of the Subcommittee, thank you for the invitation to appear before you today to provide the subcommittee details on the actions the Department has taken or will take to strengthen the security of the nuclear weapons complex in the wake of the July 2012 Y-12 incident. We appreciate the interest and engagement of this Committee and recognize the important oversight role that you fulfill. We also share the Committee's commitment to assure that all of our offices and operations are delivering on our mission safely and securely— from Washington, DC, to California, from every naval reactor to every warhead, from production to clean-up, from deterrence to nonproliferation.

**Introduction**

Since its creation in 1999, the National Nuclear Security Administration (NNSA) has served as a separately-organized entity within the U.S. Department of Energy, entrusted with the execution of our national nuclear security missions. Living up to the challenging demands of executing our mission safely, securely, and in a fiscally responsible manner requires daily management through strong, effective, and efficient relationships with our Management and Operating (M&O) contractors.

The protection of all Department of Energy (DOE) people and assets — our federal and contractor employees, technology, and physical assets, including both nuclear and non-nuclear facilities and other resources — is of integral importance to our mission. The Secretary and I know that, and understand our responsibilities to that mission, in its entirety. Indeed, we have reflected our commitment through our Management Principles, which provide that:

- We will treat our people as our greatest asset;
- We will pursue our mission in a manner that is safe, secure, legally and ethically sound, and fiscally responsible; and
- We will succeed only through teamwork and continuous improvement.

The Secretary has expressed a consistent, unwavering commitment to maintain safe and secure work environments for all Federal and contractor employees. In that spirit, we are determined to assure that the Department's and contractors' operations do not adversely affect the health, safety, or security of workers, the surrounding communities, or the Nation.

DOE's mission includes diverse operations, involving a variety of nuclear materials and processes. We recognize our unique obligations as a self-regulated agency to establish and meet exacting standards for nuclear safety and security, to maintain robust nuclear safety performance, and to provide rigorous and trustworthy oversight and enforcement of those nuclear safety and security standards. We must also maintain a safety and security culture that values and supports those standards, and assures that individuals can freely step forward to voice their concerns related to our safe execution of our mission. Indeed, we encourage them to do so. Only through these actions can we provide adequate protection of our workers, the public, and the environment, while sustaining the public trust and confidence crucial to our ability to fulfill the mission.

To achieve our mission, DOE must strive to excel simultaneously as a self-regulator, as an owner, and as an operator of the facilities in our national security complex. Each of these roles is vital and must be executed with integrity. The July 2012 incident at Y-12, as the Secretary and I have repeatedly emphasized, was unacceptable, and we have taken and will continue to take steps not only to identify and correct issues at that site, but across the DOE complex. I will address the Department's response to the incident in more detail later in this testimony.

**Roles and Responsibilities for Nuclear Security within DOE**

The Secretary and I bear ultimate responsibility for nuclear safety and security at DOE facilities. Under our direction, line managers have the authority and the responsibility for establishing, achieving, and maintaining stringent performance expectations and requirements among all Federal and contractor employees, at DOE labs and other facilities.

The Department's Office of Health, Safety and Security (HSS), in consultation with line management, is responsible for the development of DOE nuclear safety and security policy, Federal Rules, Orders, and the associated standards and guidance, as well as for reviewing safety and security issues complex-wide. HSS also conducts independent oversight and regulatory enforcement that is independent from line management. HSS oversight has expanded the scope and variety of performance testing methods utilized to assess the readiness of DOE and NNSA site protection systems against a defined spectrum of threats and adversary capabilities Performance testing methodologies include no-notice and limited notice inspections to obtain a more realistic assessment of site response capabilities and readiness performance.

The Department's approach to nuclear safety and security is founded on a demanding set of standards that capture knowledge and experience in designing, constructing, operating,

deactivating, decommissioning, and overseeing nuclear facilities and operations. DOE applies validated national and international standards to the maximum extent possible, because these standards reflect broad input from a large and diverse group of experts. As our management principles state: "We will apply validated standards and rigorous peer review."

Our management principles also require that we "manage risk in fulfilling our mission." This is essential to a robust safety and security culture, as demonstrated by the 2010 Deepwater Horizon oil spill, which vividly demonstrated the inadequacy of a mere "check-the-box" mentality by regulated entities when it comes to smart decision-making in a complex and hazardous operational environment. Since DOE expects scrupulous compliance with its requirements, managers and workers must recognize and embrace their personal accountability to meet safety standards, while avoiding a tendency for rote compliance with requirements. In some cases, it may be necessary to raise a hand and ask if another approach could offer a smarter way to assure safety. This questioning attitude must be encouraged.

Finally, the Secretary and I are also dedicated to strengthening contract and project management. Indeed, we cannot succeed in advancing our goals for the Department if we fall short in this effort. And, as we all know, safety and security are integral to effective contract management. Indeed, safety and security are key performance standards and elements of every contract, and extensive oversight is required to ensure stewardship as well as legal and regulatory requirements are met. When we have a safety or security problem, we must fix it, which may lead to increased costs and delays. So building safety and security into the fabric of our programs and our projects from the start and continuously monitoring adherence to safety standards is not just the right thing to do from a moral perspective, and not just the necessary thing to according to our governing laws and regulations, but it is also the smart thing to do, as stewards of our responsibilities to the Nation and its taxpayers.

**Response to Y-12 Incursion Incident**

On Saturday, July 28, 2012, at 4:30AM three individuals trespassed onto the Y-12 National Security Complex and defaced a building at NNSA's Y-12 National Security Complex in Oak Ridge, Tennessee.

This incursion and inadequate response to it demonstrated a deeply flawed security culture and equally flawed execution of security procedures at Y-12. In response to the incident, we acted swiftly to identify and address the problems it revealed.

Since the Y-12 incursion, several major actions have taken place to improve security:

*Federal and Contractor Management Changes*

New senior Federal and contractor management personnel were brought in to take charge of Site and Headquarters organizations, to transform our approach to security. Of the Federal personnel, a highly-experienced individual was appointed to serve as the new Chief of Defense

Nuclear Security and to develop overall policy; two Federal office directors experienced in security matters were appointed to implement the new policies. Of the contractor management personnel, a new M&O Site Manager and the top security official were appointed by the contractor to implement the vital security transformation.

*IG Inquiry into Y-12 Security Breach*

The Department and NNSA have been working diligently to implement the recommendations of the August 2012 IG report, including verifications that all critical security equipment at Y-12 has been repaired and is operational.

*Protective Force Contract Terminated, New M&O Contractor Selected*

WSI's protective force contract was terminated and a new M&O contactor has been selected to manage the Y-12 site, providing an opportunity for new leadership and to improve Y-12's security culture and management. On January 8, 2013, the NNSA awarded a contract worth $23 billion over 10 years to Consolidated Nuclear Security (CNS) for the combined management of the Y-12 National Security Complex in Tennessee and the Pantex Plant in Texas, with an option for phase-in of Tritium Operations performed at the Savannah River Site in South Carolina. The award is currently under an automatic stay while being protested at the GAO. Combining contracts and site offices will allow us to improve performance and operate as an integrated enterprise.

*HSS Y-12 Security Inspection*

HSS conducted an independent security inspection of Y-12 security operations, which included rigorous force-on-force performance testing as well as no-notice and short-notice limited scope performance testing activities as directed by the Secretary. The final report of inspection results was completed and briefed to senior management on September 28. The Y-12 inspection results were also briefed to Congressional staff. HSS will be conducting a follow-up review in April to examine the status of implementation of corrective actions.

*Extent of Condition Reviews*

At the direction of the Secretary, the Department's Chief of Health, Safety and Security also conducted extent of condition reviews at all of the DOE and NNSA Category I Special Nuclear Material (SNM) sites in collaboration with DOE and NNSA Program Offices. These reviews assessed the current security posture, specifically to determine whether the systemic issues identified at Y-12 were present at other sites, so that any necessary steps could be taken to cure any such defects. HSS completed its review in December 2012. The results were briefed to DOE leadership and Congressional staff.

*Comprehensive Independent Oversight Security Inspections of all Category I Sites*

The Secretary also directed HSS to conduct assessments of all Category I sites across the DOE complex, to identify any systemic security issues. These deep dives are being conducted by the HSS Independent Oversight organization, and include the HSS enhanced program of performance testing program, evaluation of force-on-force exercises, no-notice security testing, and comprehensive security inspections at all Category I sites by October 2013. HSS has completed security inspections at Y-12, Oak Ridge National Laboratory and the Hanford Site. Results of these inspections have been briefed to DOE leadership and Congressional staff. The remaining security inspections will include the Savannah River Site (field work completed February 21), Pantex Plant, Idaho National Laboratory, Office of Secure Transportation, the Nevada National Security Site, and Los Alamos National Laboratory.

*Independent Expert Panel Review of Y-12*

Secretary Chu requested three former senior executives from Federal agencies and the private sector to conduct a strategic review of the entire DOE security architecture with a particular emphasis on Y-12. These executives included President of the Carnegie Foundation and former Nuclear Regulatory Commission Chairman Richard Meserve, former Lockheed Martin CEO Norman Augustine, and retired Air Force Major General Donald Alston. Each one provided thoughtful advice on the DOE's nuclear security structure, specifically all Category I nuclear facilities. Their words of advice and ideas are current being considered to improve security at Y-12 and across the nuclear enterprise.

*Brigadier General Sandra Finan's Review*

On August 14, 2012, then NNSA Administrator Tom D'Agostino commissioned a Security Task Force led by Brigadier General Sandra Finan to analyze the then-current federal NNSA security organizational structure and security oversight model, and to recommend possible improvements.

Over the course of several months, Gen Finan and the members of the Task Force conducted a thorough review of NNSA security operations at headquarters and in the field.

Organizational Improvements

Prior to the Y-12 incursion, the Headquarters NNSA security organization, the Office of Defense Nuclear Security (NA-70), served as a "Functional Manager" for the security mission, while the line authority flowed from the Secretary to other NNSA Administrators and other organizations. General Finan recommended for strategic-level policy guidance, requirements determination, and performance assessment to be under the jurisdiction of the Chief, Defense Nuclear Security (NA-70). NNSA's Office of the Associate Administrator for Infrastructure and Operations (NA-00) would provide the operational accountability for NNSA's security organization. Operational

implementation and standardization of operations across the security program occurs at the NA-00 level.

The existence of a single point through which the field reports and is held accountable is the way the NNSA will assure the consistent and effective implementation of security policy. This is a change from the approach the NNSA has taken—where each field office had greater latitude in implementing policies and requirements for its site.

Additionally, Gen. Finan made recommendations to eliminate the conflict between DOE Security Orders and NNSA NAPs. Specifically, NNSA should use DOE Security Orders. DOE has a specialized security policy function that produces its orders. Rather than attempt to duplicate this function, DOE orders would provide direction while the NAP process would provide guidance and clarify information in the orders as appropriate, but not reduce requirements.

Changing the Assessment Model

Regarding NNSA's security oversight model, Gen. Finan found that at the time of the Y-12 incursion NNSA did not have an adequate security performance assessment process or capability. The systems-based assessment model that was employed was ineffective for security. NNSA lacked a clear and consistent performance baseline for security program implementation and the assessment model was biased against criticism.

To directly address problems with the assessment model, NNSA has set about implementing a three-tiered approach to assessing security throughout the NNSA. This approach includes: 1) an initial assessment performed by the contractor at the site, 2) an assessment of the contractor's performance carried out by the Chief of Defense Nuclear Security at DOE Headquarters (NA-70), and 3) independent oversight by the Office of Health, Safety and Security. And, of course, apart from this three-tiered assessment and inspection regimen, we expect Federal site personnel to perform quality assurance activities on a routine basis as an integral part of their line management responsibilities.

The Secretary and I are pleased that the NNSA has responded to Gen Finan's recommendations seriously and is on a course to implement effective security improvements.

The series of personnel and management changes I have described today were made to provide effective security at the site and across the DOE complex. We are also working to carry out the structural and cultural changes required to secure all CAT 0/1 nuclear materials at this and all other DOE and NNSA facilities.

**Conclusion**

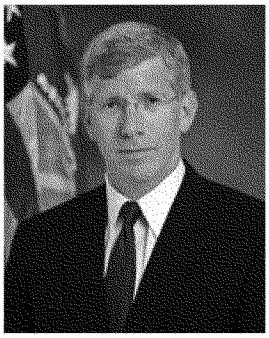
In conclusion, the security of our Nation's nuclear material and technology is a central responsibility of the Department, in support of the President and in defense of the Nation. We must remain vigilant against error and complacency and have zero tolerance for security

breaches at our Nation's most sensitive nuclear facilities. The incident at Y-12 was unacceptable, and it served as an important wake-up call for our entire complex. As a result, the Department is carefully reviewing security at all of our NNSA sites – as well as all of the recommendations of the HSS security review teams, Brigadier General Finan, DOE IG, and independent reviews provided by the distinguished panel of military and private sector experts – with a view to taking all those steps that are needed to protect this Nation's most sensitive materials and technologies. The Department is taking aggressive actions to ensure the reliability of our nuclear security programs across the entire DOE enterprise, and will continue to do so.

We accept the responsibility that we have inherited from the generations of Americans going back to the Manhattan Project to assure the safe and secure stewardship of our nuclear enterprise in order to deter aggression, defend our freedom, and support our allies.

In that effort, the Department looks forward to working with the Committee to ensure the security of the nation's nuclear materials. I would be pleased to answer any questions from members of the Subcommittee.

## DANIEL B. PONEMAN
## DEPUTY SECRETARY OF ENERGY



Daniel B. Poneman was nominated by President Obama to be Deputy Secretary of Energy on April 20, 2009, and was confirmed by the United States Senate on May 18, 2009. Under the leadership of Secretary of Energy Steven Chu, Mr. Poneman also serves as Chief Operating Officer of the Department.

Mr. Poneman first joined the Department of Energy in 1989 as a White House Fellow. The next year he joined the National Security Council staff as Director of Defense Policy and Arms Control.

From 1993 through 1996, Mr. Poneman served as Special Assistant to the President and Senior Director for Nonproliferation and Export Controls at the National Security Council. His responsibilities included the development and implementation of U.S. policy in such areas as peaceful nuclear cooperation, missile technology, space-launch activities, sanctions determinations, chemical and biological arms control efforts, and conventional arms transfer policy. During this time, he also participated in negotiations and consultations with governments in Africa, Asia, Europe, Latin America, and the former Soviet Union.

After leaving the White House, Mr. Poneman served as a member of the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction and a number of other federal advisory panels.

Prior to assuming his responsibilities as Deputy Secretary, Mr. Poneman served as a principal of The Scowcroft Group for eight years, providing strategic advice to corporations on a wide variety of international projects and transactions. Between tours of government service he practiced law for nine years in Washington, D.C. - first as an associate at Covington & Burling, later as a partner at Hogan & Hartson - assisting clients in regulatory, policy and transactional matters, international arbitration, commercial real estate financing, export controls, and sanctions and trade policy.

Mr. Poneman received A.B. and J.D. degrees with honors from Harvard University and an M.Litt. in Politics from Oxford University. He has published widely on national security issues and is the author of Nuclear Power in the Developing World and Argentina: Democracy on Trial. His third book, Going Critical: The First North Korean Nuclear Crisis (coauthored with Joel Wit and Robert Gallucci), received the 2005 Douglas Dillon Award for Distinguished Writing on American Diplomacy. Mr. Poneman is a member of the Council of Foreign Relations.

Mr. Poneman lives in Virginia with his wife, Susan, and their three children.

## DOCUMENTS SUBMITTED FOR THE RECORD

FEBRUARY 28, 2013

## DOE Verbal Shortcuts and Acronyms

The following acronyms and shortcuts are used at DOE to quickly identify people and offices:

People:

| | |
|---|---|
| S-1: | Secretary of Energy |
| S-2 or DS: | Deputy Secretary of Energy |
| ADS: | Associate Deputy Secretary of Energy |
| S-3: | Under Secretary (sometimes referred to as Under Secretary of Energy) |
| S-4: | Under Secretary for Science |
| NA-1: | Under Secretary for Nuclear Security, and Administrator for NNSA |
| U/S: | Under Secretary abbreviation |
| Dash 1s: | Assistant Secretaries/ Program Element Heads (For example, FE-1 is the Assistant Secretary of Fossil Energy.) Dash 1s can also be PSOs or Program Secretarial Officers. Dash 1s are generally political appointees except for PMAs and LM, and several staff and support offices (CIO, HG, HSS, ED and MA). |
| PDAS: | Principal Deputy Assistant Secretary (generally, the most senior career employee) |
| DAS: | Deputy Assistant Secretary (generally, a senior career employee) |
| PAS: | President Appointed/Senate |

**Confirmed Program Offices/Administrations:**

EERE: Office of Energy Efficiency and Renewable Energy
FE: Office of Fossil Energy
NE: Office of Nuclear Energy
OE: Office of Electricity Delivery and Energy Reliability
IE: Office of Indian Energy Policy and Programs
ARPA-E: Advanced Research Projects Agency – Energy
PMAs: Power Marketing Administrations
EIA: Energy Information Administration
LPO: Loan Programs Office
SC: Office of Science
NNSA: National Nuclear Security Administration
EM: Office of Environmental Management
LM: Office of Legacy Management

**Staff and Support Offices**

CFO: Chief Financial Officer
CHCO: Chief Human Capital Officer
CIO: Chief Information Officer
CI: Congressional and Intergovernmental Affairs
ED: Economic Impact and Diversity
GC: General Counsel
HSS: Health, Safety and Security
HG: Hearings and Appeals
IG: Inspector General
IN: Intelligence and Counterintelligence
MA: Management
PI: Policy and International Affairs
PA: Public Affairs

## NNSA KEY PERSONNEL

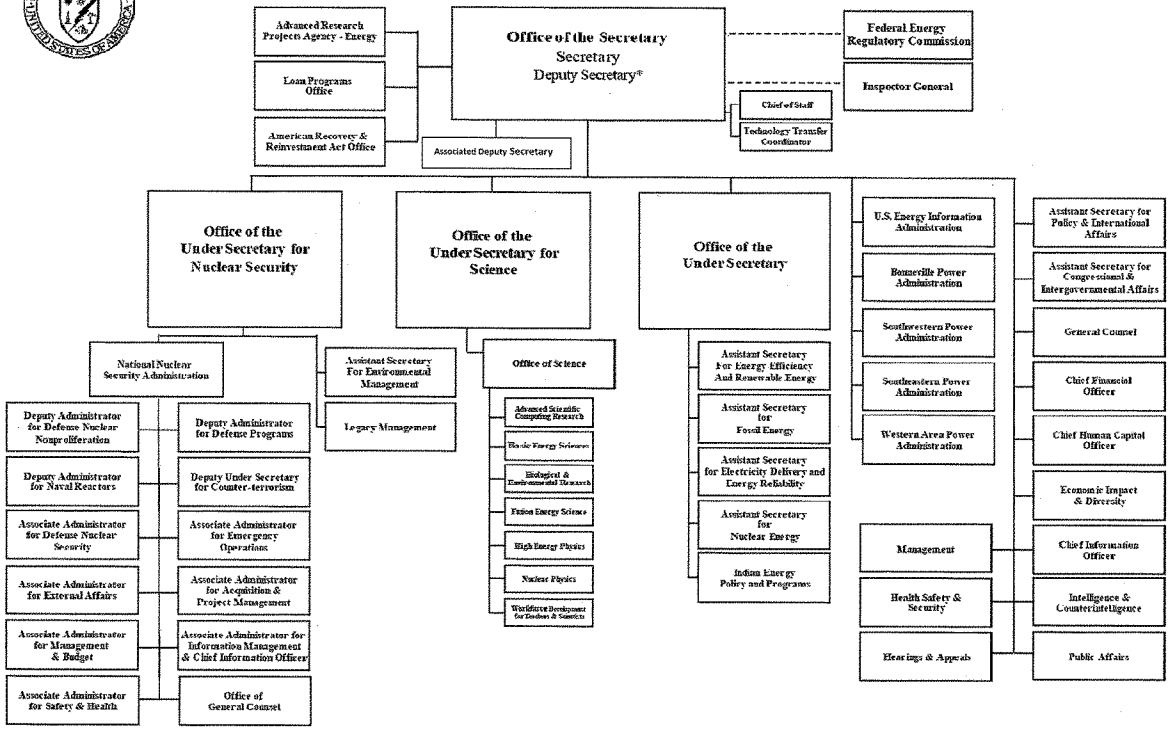
The following individuals are the Presidentially-appointed, Senate Confirmed NNSA personnel

- Neile Miller, Acting Under Secretary for Nuclear Security and Administrator
- Neile Miller, Principal Deputy Administrator
- Donald Cook, Deputy Administrator for Defense Programs
- Anne Harrington, Deputy Administrator for Defense Nuclear Nonproliferation
- Admiral John Richardson (USN), Deputy Administrator for Naval Reactors

The following individuals are the Senior Executive Service personnel that lead mission and mission support functions:

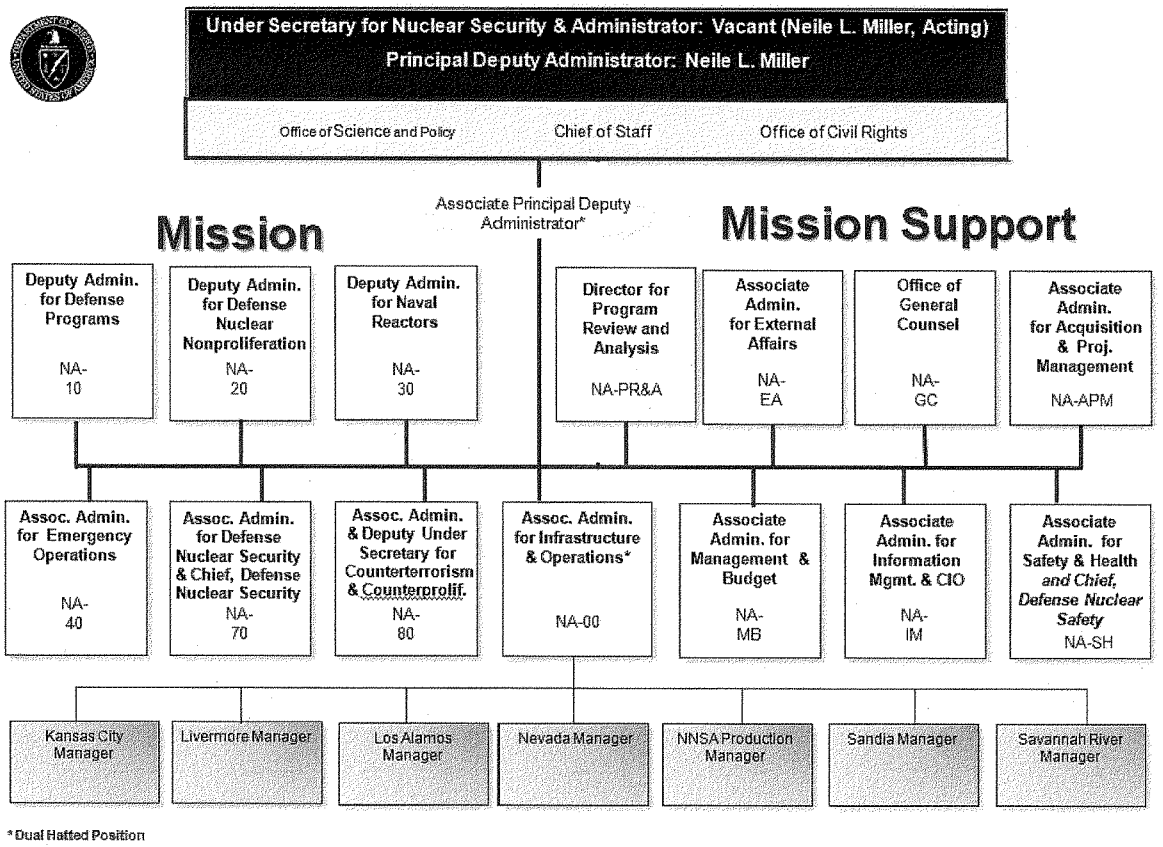
- Michael Lempke, Associate Principal Deputy Administrator and Associate Administrator for Infrastructure and Operations (NA-00)
- Robert Raines, Associate Administrator for Acquisition and Project Management (NA-APM)
- Joseph Krol Jr., Associate Administrator for the Office of Emergency Operations (NA-40)
- Dimitri F. Kusnezov (Acting), Associate Administrator for Information Management & CIO (NA-IM)
- Bruce Diamond, General Counsel (NA-GC)
- Clarence T. Bishop, Associate Administrator for External Affairs (NA-EA)
- Dr. Steven Aoki, Associate Administrator for Counterterrorism and Counterproliferation (NA-80)
- Steve Asher (Acting), Associate Administrator for the Office of Defense Nuclear Security (NA-70)
- Don Nichols, Associate Administrator for Safety and Health (NA-SH)
- Cindy Lersten, Associate Administrator for Management and Budget (NA-MB)
- Steve Ho, Director for Program Analysis and Evaluation (NA-PR&A)

# DEPARTMENT OF ENERGY




* The Deputy Secretary also serves as the Chief Operating Officer

25 Jul 12


Under Secretary for Nuclear Security & Administrator: Vacant (Neile L. Miller, Acting)
Principal Deputy Administrator: Neile L. Miller
Office of Science and Policy
Chief of Staff
Office of Civil Rights
Associate Principal Deputy Administrator*
Mission
Mission Support
Deputy Admin. for Defense Programs NA-10
Deputy Admin. for Defense Nuclear Nonproliferation NA-20
Deputy Admin. for Naval Reactors NA-30
Director for Program Review and Analysis NA-PR&A
Associate Admin. for External Affairs NA-EA
Office of General Counsel NA-GC
Associate Admin. for Acquisition & Proj. Management NA-APM
Assoc. Admin. for Emergency Operations NA-40
Assoc. Admin. for Defense Nuclear Security & Chief, Defense Nuclear Security NA-70
Assoc. Admin. & Deputy Under Secretary for Counterterrorism & Counterprolif. NA-80
Assoc. Admin. for Infrastructure & Operations* NA-00
Associate Admin. for Management & Budget NA-MB
Associate Admin. for Information Mgmt. & CIO NA-IM
Associate Admin. for Safety & Health and Chief, Defense Nuclear Safety NA-SH
Kansas City Manager
Livermore Manager
Los Alamos Manager
Nevada Manager
NNSA Production Manager
Sandia Manager
Savannah River Manager
* Dual Hatted Position

**WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING**

FEBRUARY 28, 2013

## RESPONSE TO QUESTION SUBMITTED BY MR. COOPER

Mr. PONEMAN. The average gross wages and fringe benefits for a guard or Protective Force member at Y–12 is $88,000. Actual take home pay will vary by individual based upon payroll deductions and hours worked. [See page 30.]

---

## RESPONSE TO QUESTION SUBMITTED BY MR. GARAMENDI

Mr. PONEMAN. Please find attached an organization chart of both organizations. We've also included the names of the key NNSA leadership team. [See page 26.]

[The information referred to can be found in the Appendix beginning on pages 111–114.]

## QUESTIONS SUBMITTED BY MEMBERS POST HEARING

FEBRUARY 28, 2013

## QUESTIONS SUBMITTED BY MR. ROGERS

Mr. ROGERS. General Alston, you recognized human capital limitations as a contributing factor to the event. What can Congress do, if anything, to enhance human capital at NNSA as it pertains to security?

General ALSTON. Recognizing that the July 2012 Y–12 security failure had more to do with ineffective oversight and a culture that readily accepted security deficiencies rather than human capital weaknesses, it's my view that NNSA and DOE did not assign sufficient value to security expertise when it made staffing decisions. As a result, there is no ready pipeline of leaders with appropriate security expertise. This condition is exacerbated by personnel practices that did not circulate security leaders between the HQ and the sites.

The quality of experience and expertise across our national nuclear enterprise has been an area of increasing concern, perhaps since the end of the Cold War. The Congress in the 1997 and 1998 National Defense Authorization Acts established a Commission on "Maintaining United States Nuclear Weapons Expertise," led by ADM (ret) Hank Chiles. ADM Chiles led a similar Defense Science Board effort in 2008. Neither of these efforts highlighted nuclear physical security expertise as a focus area, but they emphasize the overall importance of expertise throughout the nuclear enterprise. All other things being equal, I personally would be inclined to hire someone who has secured nuclear materials before I would hire one without that background. The size of our nuclear enterprise continues to expose a keen personnel vulnerability across all disciplines that should be driving focused human capital development plans. The benefits include good daily operations, strong crisis management competencies at upper levels and a self-sustaining community of experts.

Mr. ROGERS. General Alston, do you, Mr. Augustine, and Dr. Meserve believe the confused lines of responsibility and authority for security are just within NNSA, or do they extend to security and leadership organizations within DOE as well?

a. You are your fellow reviewers have suggested that security operations with DOE and NNSA need to be reorganized in order to re-align authority and responsibility. What guidelines should be followed in aligning and assigning authority and responsibility? Is it your sense that these guidelines are being followed?

General ALSTON. The confused lines of responsibility and authority for security at the time of our project were within the contractor relationships at the sites, NNSA and DOE.

a. Match authority and responsibility at the right level.

—For example, at Y–12, the site Maintenance and Operations contractor was responsible for security infrastructure, such as security camera maintenance, while the security contractor was responsible for providing ready protective forces. This split responsibility for security tools and security pros contributed to the atmosphere that tolerated enduring infrastructure deficiencies.

—Additionally, empower the NNSA rep overseeing site security with sufficient authority to hold him/her accountable appropriately for local performance failures, as necessary.

—Finally, establish who is accountable at the headquarters level for day-to-day security operations. Who is accountable to track and eliminate security deficiencies? Who is accountable for security system developmental and operational testing? To name just a few critical elements we had trouble resolving during our study.

Scrub department governance and eliminate inadequate, conflicting and redundant sources of security policy.—For example, securing Category 1 material at SRS should require the same measures as securing Category 1 material at Y–12.

Establish clear organizational lines from the field through the senior levels at the headquarters that not only enable the two points above, but also focus on ensuring effective 2-way communication throughout the organization.

I do not have a sense whether or not these guidelines are part of DOE/NNSA security initiatives.

Mr. ROGERS. General Alston, your letter to Secretary Chu says "there is a perception that corporate security policy is being written from inspection results." Mr. Augustine noted that inspections and assessments inappropriately focus on compliance with standards, and not on security effectiveness or performance. He concluded that

"what is needed is not more inspections but better inspections." Do you agree with Mr. Augustine on this point?

a. To what extent do you believe that oversight activities should also be standardized and/or centrally directed?

b. Would you please compare and contrast how the Department of Defense conducts inspections and writes security policy with how DOE and NNSA do?

c. How should oversight of security operations be conducted? How would you modify the DOE/NNSA inspection and oversight approach to make it better?

General ALSTON. I absolutely agree with Mr. Augustine. Well-focused inspections, at smart intervals, consistently and appropriately evaluating compliance and performance against clearly established standards provide both local leadership and NNSA and DOE "snapshot" indicators of site competency. As a part of a comprehensive set of indicators that include daily performance metrics, resourcing levels, and several more elements to complete the readiness picture, a sound inspection process is vital.

a. Independent oversight of activities involving nuclear materials is essential due to the extraordinary safety, security and geopolitical nature of nuclear weapons and related components. High standards are established and their compliance must be verified. The most senior accountable overseer must have the means to assure subordinate elements are in compliance with standards and can perform critical aspects of the mission. Therefore, the Secretary of Energy requires an independent inspection apparatus. The NNSA Administrator also needs to ensure compliance with these same high standards. Whether or not the Administrator of this semi-autonomous agency requires his/her own independent inspection apparatus should be evaluated.

Common standards must be applied in a common way in the field and must be inspected in a common way by the inspection team. This has the benefit of enabling senior leaders to calibrate compliance, preparedness and overall competency through inspection results they can have confidence in. Additionally, consistent inspections should serve the purpose of reinforcing universal expectations by field elements that clear standards will be evaluated in consistent ways. Without consistency in evaluation, trust can break down between the HQ and the field and sites will fear the next inspection will be less about standards and more about inspection team whim. Unjustified policy revisions can also creep into the process as a result of poorly organized and executed inspections.

b. The DoD depends both on the Services and the Defense Threat Reduction Agency to conduct inspections. The vast majority of nuclear expertise is created at the operating unit level and from this initial development, the substantial oversight demand signal is generated by Inspector General teams at every nuclear Major Command in the AF (that would be 5 AF IG teams, plus the AF Inspection Agency), plus, the Services feed nuclear expertise to DTRA and Combatant Commander inspection organizations (small though they may be). I lack personal experience to discuss Navy processes, so I'll stick to the AF. Nuclear-related policy is written at the Office of the Secretary of Defense level by functional experts and that policy is applied to the AF at the Air Staff level by the AF functional experts: personnelists, manpower, intelligence, operations, logistics, supply, security, medical, etc. Functional experts at both the Air Staff and the Major Command level establish what should be inspected and go so far as to write the checklists that are issued to the inspection teams. The AF performs a variety of inspections that affect nuclear-equipped units, but the most relevant nuclear-related inspections include the Nuclear Surety Inspection and the Operational Readiness Inspection. Both types have compliance and performance-based elements. Additionally, subordinate units have self-inspection processes, local exercises, written and oral tests. Strategic Command also conducts major large scale exercises.

Our relatively short duration study of security across DOE did not afford us the opportunity to examine DOE and NNSA policy formulation or inspections in great detail. We did have difficulty understanding how these processes worked in practice. We noticed security policy being written both inside and outside NNSA, suggesting a need to validate the appropriateness of multiple security governance tracks, especially where the result potentially drove different security applications in the field at different locations.

The record shows the DOE had inspected Y–12 just prior to the July 2012 incident and despite extensive documented evidence of an imminent train wreck, Y–12 got good grades. Clearly DOE was not looking at the right things, or lacked sufficient security competency to recognize the existing failure conditions. Beyond IG-type inspections, system readiness/acceptance testing is also relevant to this question. As Mr. Augustine said when discussing operational testing of security systems, "... tests have too often addressed the question, 'Does the hardware or practice meet

the design criteria rather than is it operationally effective?' Standards are often procedural rather than performance-oriented, and stress testing has been lacking."

c. Scrub governance to validate Department and Agency requirements and eliminate conflicting or inadequate guidance. Then, ensure productive alignment of authority and responsibility to produce policy and ultimately oversee effective current operations and prepare for tomorrow's effective operations. These two steps will help set the conditions for a value-added inspection process that can produce dependable results for local and headquarters awareness and action, as appropriate.

Mr. ROGERS. General Alston, in your letter to Secretary Chu, you note that metrics are an important complement to inspections as part of a comprehensive oversight program (Dr. Meserve made the same point). Reviews of the Y–12 incident have found that very few performance metrics were tracked by contractors and NNSA. What high-level metrics should we be tracking as Members of Congress to ensure that the security program is operating effectively?

a. What are the most important metrics for senior officials to be tracking to assurance robust security performance?

b. In addition, how can NNSA leadership ensure that "quality metrics" are developed and used by Federal staff and contractors to conduct oversight?

c. How many metrics is too many—at what do the important ones get lost in the noise?

General ALSTON. a. All are related to understanding risk and being able to competently accept risk up the chain. Metrics could include:

Resource limitations driving non-standard activities. (personnel shortages driving overtime; parts availability driving prolonged outages of security equipment and extended implementation of compensatory measures)

Safety incidents. Number, quality, trends.

Security incidents. Number, quality, trends.

Progress on security system modifications or upgrades.

Inspection results.

Inspection deficiency follow-up/resolution.

b. I think the metrics are chosen by identifying those governance requirements that spell 'mission failure' if ever breached. Additionally, metrics should be collaboratively identified throughout the chain of command. Authentic desire for site input goes a long way towards achieving corporate buy in to these important measurements.

c. Good question. I think some metrics are very relevant to the NNSA Administrator, and at the same time, more detailed subordinate metrics might be more appropriate at the local level. It's important to get the right information to the person accountable to fix the problem. In addition to just pushing data up the chain, it is perhaps more important for this content to drive interaction up and down the chain to reinforce constant leadership commitment to security, and for site participants to take that leadership commitment evidence to all the personnel on site.

Mr. ROGERS. General Alston, your letter indicates serious problems with the security culture at NNSA and DOE, and that many of these problems have existed for decades.

a. Can we change the security culture without some sort of fundamental changes? Is it possible to shift the culture using only incremental changes?

b. Culture changes are extremely difficult and often take a long time—what immediate-term actions should we be taking to begin this needed culture shift?

c. You recommend federalizing the security forces. Do you think that would a large enough change to shift the culture?

General ALSTON. a. In my experience, when culture change is needed, incremental adjustments will either fail to achieve the required change or will not drive change at the necessary speed.

b. If the need for culture change is legitimized, dramatic action is often a catalyst for changing culture. A change in leadership, a clear articulation of the vision and the need for the change, sometimes a major re-organization are all relevant considerations. Key to setting conditions for change is to reinforce the value of security in NNSA and DOE and that is achieved in large part with accountability. Overcommunicate the standards and expected performance levels and consistently enforce them. Mr. Augustine identifies 7 ingredients to successful culture change on page 4 of his 6 December 2012 letter to Dr. Chu.

c. No, federalizing the NNSA protective forces alone will not achieve the necessary culture change. Without the proper alignment of authority and responsibility up and down the chain between the sites and the HQ and without an effective means to ensure all members of NNSA and DOE understand their individual roles in security, all the necessary pieces will not be in place and the conditions will not have been set. However, federalizing the protective forces not only makes operational

sense, but it would be a clear expression of intent and institutional commitment that, in my view, would be worth the cost in the long run.

Mr. ROGERS. General Alston, you and Mr. Augustine and Dr. Meserve seem to have read the many reports and independent reviews of DOE security that have been conducted previously. Your letter to Secretary Chu calls it "the considerable body of work that has been done on this subject over the past decade." In particular, you mention the review done by Admiral Mies in April 2005. In my opening statement, I mentioned a few others—but there are many, many more.

How do your findings and recommendations compare with those contained in all of these previous reports? Do you feel the findings and recommendations in the previous reports have been acted upon and addressed?

General ALSTON. It is my view that many of the past reports contain observations and recommendations that also seemed relevant during the time of my study. In my opinion, the broadest security examination was led by ADM (ret) Mies and for that reason I encouraged the Secretary of Energy to critically re-evaluate DOE/NNSA documented resolution of that report's set of recommendations. Though I did not audit all the relevant reports in response to this QFR, I did review the Mies report again. I have included below some of the Mies recommendations that echoed with what I was observing at the time of my study. I suspect DOE/NNSA has taken relevant action in response, but given what I observed, continued vigilance is required.

Some still-resonating Mies recommendations:

- "Continue to promote greater collaboration and team building within NNSA with the goal of an enterprise approach to security. Support the Chiles panel recommendations on improved career development, assignment rotation training, professional qualification and certification, etc.
- Make an unequivocal commitment to upgrade the quality, relevance, and ownership of security training programs and professional certification.
- Emphasize a balance of compliance and performance objectives designed to incentivize and embed security improvement throughout NNSA, as part of an enterprise approach to security.
- Create a stronger climate of trust in the security program. Differentiate honest human security errors from malicious, grossly negligent ones.
- Adopt a more proactive approach to security through stronger accountability.
- Conduct an independent staffing assessment of NNSA relative to DOE. Rebalance staffing and expertise commensurate with the significance of the national security assets NNSA manages.
- Give greater autonomy and authority to the NNSA Administrator to oversee the elements of the security process, from policy formulation to implementation and oversight, which directly affect security of the NNSA complex.
- Implement the recommendations of the Chiles report to improve the federal security workforce, including developing and executing a comprehensive human capital management program; improving the training, qualifications, and stature of the NNSA security workforce; reengaging in national markets to hire security professionals; instituting a long-term practice of security staff rotation; identifying options for accelerating the security clearance process; improving security information flow; revising the NNSA Safeguards and Security Strategic Plan; and providing specific budget support for and tracking the progress of these recommendations.
- Continue to elevate security program visibility and importance through initiatives such as the June 2004 organizational realignment, to ensure security is commensurate with other line management responsibilities.
- Have NNSA headquarters assume greater responsibility for day-to-day supervision and oversight of site activities to promote an enterprise-wide approach to security, more consistent interpretation of security policy, and more standardized and coherent implementation. The new Associate Administrator for Defense Nuclear Security should be assigned responsibility for day-to-day security oversight. Responsibility for implementation needs to reside at all levels.
- Establish formal mechanisms to enable DOE/NNSA to regularly collaborate with DoD (and other appropriate federal agencies) on security policy issues, lessons learned, best practices, technological improvements, tactics, and procedures as recommended by a previous study.
- Promote greater reliance on continuing security self-assessment programs to better inculcate security as every individual's responsibility and integral to mission.
- Consider changing the annual survey and self-assessment program to a year-round program of in-depth assessments in specific areas.
- Formulate an NNSA-wide strategic security plan, similar in level of detail and content to DOE's, to create a unifying security roadmap for the NNSA enter-

prise. Use this plan as a cornerstone for the creation of other interdependent enterprise wide plans, such as special nuclear material consolidation, infrastructure recapitalization, technology investment, information systems modernization, and the foundation for individual security discipline plans (physical, cyber, personnel, and material control and accountability).

- Establish effective, formal forums to: promote greater DOE/NNSA-to-DOD, DOE-to-NNSA, headquarters-to-site, and site-to-site collaboration between security policymakers and policy implementers, promote more consistent interpretation and application of security policy, foster adoption of best practices, help formulate a more coherent, NNSA-wide security plan, consider making peer review an inherent element of security policy formulation and implementation.
- Review and streamline local site compliance-based quick fixes to ensure security oversight is appropriately focused on performance objectives.
- Provide greater centralized clarification and interpretation of security policy to promote more consistent and standardized implementation. Consider re-promulgation of a security standards and criteria manual.
- Consider conducting random testing of the PF throughout the year in both firearms and physical fitness. This testing will encourage officers to maintain weapons skills and physical fitness levels year-round and will give management a more realistic picture of the overall PF's capabilities.
- Direct site offices to regularly check the false or nuisance alarm rates from the CAS and compare them with the credit taken in the VAs to ensure the analysis accurately reflects field conditions. Establish a method to properly record and document the false or nuisance alarm rate and ensure proper training for CAS PF personnel.
- Install modern computer alarm equipment that has an automated alarm tracking system to replace antiquated systems.
- Establish a more rigorous process within DOE/NNSA headquarters to thoroughly review initial incident reports; monitor the inquiry progress; review final reports for adequacy of the inquiry, corrective actions, and analysis of underlying causes; and keep senior DOE/NNSA leadership appropriately advised.
- Establish a more formal and disciplined process at sites to track security incident corrective actions to completion. Consider requiring site management to include findings and corrective action plans in a site-level corrective action tracking process involving senior line management to ensure corrective actions are adequate and complete.
- Ensure reviews are conducted to execute continuous improvement.
- As also recommended by the Chiles report, establish a dedicated and more effective formalized process within NNSA headquarters to disseminate incident lessons learned to the NNSA community.
- Consider publishing a quarterly lessons-learned message for all DOE/NNSA sites, with procedures for ad hoc promulgation of urgent lessons learned.
- Develop more meaningful security metrics that accurately measure the nature, frequency, and significance of incidents; the underlying root causes; and the timeliness of reporting, investigation, and corrective action development. Periodically provide these metrics to senior headquarters and site leadership, as well as appropriate security officials, to promote greater awareness of security performance and concerns.
- Consider a reasonable standardization of site security system architecture, design, and implementation, including the security upgrades in progress. NNSA site oversight and headquarters should be involved in each critical decision stage of security upgrade projects. Project rationale and justification should be scrutinized and compared with complex-wide needs and overall direction. This would optimize the use of security up-grade funding and present a clear direction for security strategy.
- Develop, with urgency, a more robust, integrated DOE/NNSA-wide process to provide accountability and follow-up on security findings and recommendations."

Mr. ROGERS. If previous studies have repeatedly noted the same problems—for instance, confused lines of authority, responsibility, and accountability—why have they not been addressed? Why have prior attempts to implement change at NNSA failed? What should Congress do to ensure these issues are addressed once and for all?

General ALSTON. Some in DOE and NNSA have pointed to the transitory nature and frequency of leadership change and a lack of continuity of priorities during these transitions as causal. It is my view that in the current DOE culture, "safety," "security," "science (labs)," and "mission (production sites)" share a common, finite tradespace and compete with each other for emphasis and resources. If there is in-

sufficient individual security expertise at the senior levels of NNSA and DOE, and no common appreciation for the value of security across senior leadership—except in crisis—security concerns will find inconsistent support and ultimately weak follow through.

Mr. ROGERS. General Finan, your report indicates serious problems with the security culture at NNSA, and that many of these problems have existed for decades.

a. Can we change the security culture without some sort of fundamental changes? Is it possible to shift the culture using only incremental changes?

b. Culture changes are extremely difficult and often take a long time—what immediate-term actions should we be taking to begin this needed culture shift?

General FINAN. a. NNSA leadership must take bold and enduring actions. Fundamental change is required within the NNSA organizational structure and in its assessment model. This, in and of itself, will not necessarily drive a change in culture. In conjunction with implementing the new structure and model, a deliberate campaign should be initiated to emphasize the importance of the security mission in strategic plans, mission statements, policy documents, and other expressions of management intent. Security must be clearly integrated with other mission elements and appropriately recognized as essential to overall NNSA mission success.

It is possible to shift culture with incremental changes. However, those incremental changes would have to be a part of a well-planned, larger campaign designed specifically to re-shape the organization and its culture. A shift in culture is not likely if change is implemented at the margins of the issues and it does not address core faults such as the confusing and ill-defined roles and responsibilities within the NNSA federal organizational structure.

b. A deliberate campaign should be initiated to emphasize the importance of the security mission in strategic plans, mission statements, policy documents, and other expressions of management intent. Security must be clearly integrated with other mission elements and appropriately recognized as essential to overall NNSA mission success. Additionally, NNSA needs to build and execute a Security Road Map that consolidates recommendations from previous reports, articulates a clear vision of where the security program is going, and charts a path forward. Document the path in a roadmap that is signed by the NNSA Administrator and follow up with action plans that have clear ownership, and status updates.

Mr. ROGERS. General Finan, you have argued that security requirements need to be better specified (for example, your report recommends that NNSA "develop and issue specific standards against which security operations are to perform and the criteria by which they will be evaluated.").

What standards, criteria, and metrics do you suggest? What metrics should senior leaders pay special attention to in order to ensure robust security effectiveness? How many metrics is too many—at what do the important ones get lost in the noise?

General FINAN. DOE had detailed standards and criteria for security operations. The last iteration of that document is a good baseline to start from. It was issued under the title "Guide for Implementation of Safeguards and Security Directives (Short Title: Safeguards and Security Standards and Criteria)" on 26 November 1993. An example of a standard and associated criterion is listed below:

Standard

Alarm Systems Testing and Maintenance: The facility conducts operability tests of the basic alarm components at least once every seven days, and performs required and necessary maintenance on the systems.

Criteria

1. Personnel testing, maintaining, or servicing alarms have access authorizations consistent with the highest classification levels being protected, unless such testing and maintenance is performed as bench services away from the protected location or is performed under the supervision of an appropriately cleared and knowledgeable custodian of the alarm-protected location.

2. Alarms bench tested or maintained by uncleared personnel away from the protected location are inspected and tested prior to installation.

3. At least once a week, the basic alarm component is tested by simulated intrusion of the alarmed area or of the protected space of an alarmed object. (Opening an alarmed portal in a manner that would cause an alarm is an adequate weekly test.) Alarms caused by the opening and closing of areas by operating personnel in the normal performance of their activities are acceptable tests when documented as tests.

4. False and nuisance alarm rate records are maintained and results are analyzed to determine alarm system performance.

5. Corrective maintenance is initiated within 72 hours of indication of failure. Compensatory measures are initiated immediately to provide equivalent detection capability when any part of the detection system is out of service and are continued until maintenance is complete.

For Metrics, NA–70 has is working some detailed metrics in their new Mission Essential Task List that will be useful in managing the protective force and should roll up to higher level metrics that can be used by senior leaders. A basic metric framework could include the major categories of System Performance, Operational Performance, Modernization, Support Services, and Predictive Indicators. System performance could include metrics such as False and Nuisance alarm rates, camera status, sensor status, etc. Operational Performance could focus on protective force training status, evaluation results, exercise performance and depth, etc. Modernization could measure the status of the security systems by monitoring the age of the significant sub-systems. Support Services could measure contract status, standardization of procedures and documentation across the NNSA complex, etc. The Predictive Indicators metric could focus on early alerting of leadership to potential issues. For example, funding status for training could indicate future proficiency; leadership security experience levels could indicate the quality of future performance and decisions, etc. These indicators would be made up of increasing levels of detail that are used by each level of management to manage security. Establishing the right level and number of metrics is difficult. A small number of high level metrics with the ability to drill down to an appropriate level to see causes and contributing factors is essential. The key is a structured process with defined business rules that are adhered to by all participants.

Mr. ROGERS. To what extent do you believe that oversight activities should also be standardized and/or centrally directed? Will more inspections necessarily equate to more effective oversight? How should oversight of security operations be conducted?

General FINAN. There is a role for standardized, centrally directed oversight as well as for individualized, tailored evaluation. At the tactical level, oversight activities should be tailored and flexible based on needs and specific performance. As the level of overseeing organization rises, the level of standardization and centralization should rise correspondingly. For example, at the tactical level, a security supervisor would want to see and evaluate the specific actions of the team members that work for him/her. Based on the supervisors knowledge of threats, skill levels, training, and site specifics, evaluation must be tailored for the specific situation. At an operational level, evaluators must see standardization of procedures and accomplishment of objectives. These evaluations would be more standardized and controlled by a central authority. At the strategic level oversight should focus on the larger context of fulfilling mission requirements. Again, this type of evaluation should be centrally directed as it is looking for performance across the enterprise.

More inspections will not equate to better performance and will not necessarily equate to effective oversight. While inspections can drive performance, they do not ensure performance. A comprehensive system of oversight is needed.

Our report proposed strengthening the role of Federal security assessment within NNSA without diminishing the legitimate need for contractors to maintain their own self-assessment capabilities or HSS to provide Independent Oversight. We called for a three-tiered assessment process.

Contractor self-assessment is the first tier in the overall assessment process. The primary audience for the contractor self-assessments should be the contractor security managers themselves, but the self-assessments should follow a consistent, program-wide format, and be made available for review at all higher levels of management. Contractors should be required to identify, report, and resolve security issues—sanctions should come when a higher level assessment uncovers problems that the contractor self-assessments fail to identify or properly address. Even when an issue is readily resolved and corrective actions are immediate, a finding should be issued and the corrective action recorded. Failure to do so inevitably hides potential negative trends. Contractor self-assessments should involve active performance testing rather than simply relying on work observation and document review—effective security performance can only be evaluated through testing. On site Federal security personnel should actively participate in this process as quality assurance for the federal government.

The fundamental purpose of Federal security performance assessment is to ensure that requirements are properly implemented. Therefore, the primary Federal assessment organization should ultimately report to the Chief of Defense Nuclear Security, who is responsible for requirements. This provides independence not only from the contractors, but also from the tactical-level Federal field staff whose necessary day-to-day interaction with contractor managers and staff risks loss of objectivity.

This enables the Chief of Defense Nuclear Security to better ensure effective implementation of NNSA security programs. Additionally, it provides feedback on performance to the operational and tactical levels.

These Federal security assessments should include performance testing of all critical elements. The assessors should issue clear findings which are to be tracked and closed in a program-wide corrective action management system. Federal assessors should also look closely at the contractor self-assessment process; "failures to identify" by the contractor self-assessment element should automatically rise to the level of significant findings.

The final tier of the assessment model should explicitly rely upon the services of an independent security oversight function, currently provided by HSS. NNSA should arrange for a regular process of comprehensive inspections. The oversight function should be encouraged to issue strong findings for matters of potential concern to the NNSA Administrator and the Secretary of Energy, and should routinely evaluate the performance of contractor self-assessments and the Federal assessment program.

Mr. ROGERS. How do we ensure robust security oversight that is not overly burdensome?

General FINAN. Much of the "burden" of oversight is caused by excessive paperwork associated with evaluating compliance. The current security assessment process in NNSA is paper-based and is heavily dependent on field office and contractor reporting. It does not include independent observation or validation of site security implementation from NNSA. As a result, NNSA is unable to validate the implementation of security policies or contractor performance of assigned missions. Large volumes of paperwork are generated each quarter in which it is nearly impossible to discern trends or significant deficiencies.

In the area of security, oversight must be about performance. Therefore, oversight should see actual performance in the form of real world activity or exercises. Some paperwork should be reviewed, such as training records, but that paper work should already exist and not be generated solely for the purpose of outside oversight. Specific standards against which security operations are to perform and the criteria by which they will be evaluated must be codified. This will ensure security professionals know what is expected and how they will be evaluated. By eliminating paperwork generated solely for the purpose of oversight and adhering to a known set of standards and criteria, security oversight should not be burdensome.

We should also resist the notion that strong performance-based standards and criteria and an equally strong insistence on stringent performance assessment and oversight inherently constitutes an excessive burden on contractors and the field. Part of the cultural challenge lies in overcoming the tendency on the part of contractors and their field level federal counterparts to assert that their local priorities and perspectives must take precedence over comprehensive and coherent, centrally-driven security program direction. A good system must take into account special local circumstances. However, NNSA's longstanding tradition has been the assertion that "the field always knows best," and that Headquarters should simply stay out of their business. Upon close examination, many complaints about "excessively burdensome HQ security oversight" are revealed as exercises in "turf protection".

Mr. ROGERS. General Finan, your report is clearly indicating frustration when it says "the most striking result of this review falls in the area of culture sustainment. It quickly became evident that the Task Force findings closely resemble those presented in numerous prior reports such as the 2005 Mies Report and the 2004 Chiles Report." Why haven't DOE and NNSA been able to address these long-standing, well-documented problems?

a. What do you recommend that we in Congress do to ensure they are actually addressed this time?

General FINAN. DOE and NNSA have not been able to attack core issues. As a result, they make marginal change around the periphery of the issue, check the box showing they have taken action, and move on to other things. Security human capital development is a good example. Security professionals in NNSA do not have a defined career path. They do not have a program for their development, and they largely see their careers with the federal government as dead ends. This issue has been repeatedly identified. As a result NNSA has taken action. They implemented a rudimentary requirement for security professionals to get some minimal training and the started a program where they brought in young leaders as a part of the leadership development program. With this in place, it was assumed that they had taken care of the Human Capital issues identified in the 2004/2005 time frame. Unfortunately, this action did not create a career path; it did not develop security professionals; it did bring in people with little or no security expertise or necessarily even an interest in security; and it did not change the belief that there was not any-

where to progress to in security. It nibbled at the margins of a core issue . . . the fact that there was no identifiable, repeatable, or executable career path for federal security professionals.

a. Ensure that NNSA builds and executes a Security Road Map that consolidates recommendations, articulates a clear vision of where the security program is going, and charts a path forward. Document the path in a roadmap that is signed by the NNSA Administrator and follow up with action plans that have clear ownership, including regular status updates. Solutions must be enduring and will require leadership dedication.

Mr. ROGERS. General Finan, you recognized human capital limitations as a contributing factor to the event, including weak staff capabilities to assess contractor performance. What can Congress do, if anything, to enhance human capital at NNSA as it pertains to security?

General FINAN. NNSA must develop a comprehensive plan for recruiting, developing, and retaining qualified security experts. NNSA needs the right federal security professionals in the right places. Individual leaders, and collectively the entire staff, must possess an appropriate skill and experience base to provide effective security program execution. Congress can specifically help by ensuring that NNSA has the ability to hire the appropriate federal security staff, both in terms of numbers and pay scale. Currently, NNSA relies heavily on support service contractors. This is partly due to limitations (perceived or real) on funding and hiring federal personnel.

Mr. ROGERS. General Finan, your task force was directed to study organizational issues within NNSA. Your tasking did not include assessing organizational issues within the broader DOE system. In the course of your investigation, did you become aware of any organizational problems related to security in the broader DOE organization, or are these problems located solely within NNSA?

a. Do you believe the security policy-making and oversight roles and responsibilities between DOE's Office of Health, Safety, and Security and NNSA are clearly defined and understood?

General FINAN. We did find evidence of similar confusion related to ambiguous lines of authority and lack of standardization in executing the security mission. As in NNSA, we found wide variations in how the federal staffs executed their oversight roles at the various sites.

a. I do not. The Task Force identified that there is no clearly articulated or consistently implemented NNSA security policy process. A major concern is the supplanting of DOE Security Orders with generic and less restrictive NNSA policies (NAPs). Additionally, the Task Force noted a desire on the part of some NA–70 senior managers to maximize separation from DOE HSS policies and activities. Within NA–70, policy and guidance are issued through a variety of formal and informal mechanisms with erratic distribution. The Task Force identified that some Federal field organizations are inconsistent in their acceptance and application of NA–70 issued policies. Finally, NA–70 policy and guidance tend to be vague resulting in widely differing interpretations by field personnel. This has resulted in additional confusion in the field as to which policies actually apply to them.

Mr. ROGERS. General Finan, your report seems to indicate that DOE and NNSA were overly focused on paperwork, and missed the warning signs that indicated a problem at Y–12. Why such focus on paperwork? How were they missing the warning signs?

a. How would you change the assessment, inspection, and oversight process to ensure the warning signs are noticed, and security performance is assured?

General FINAN. Misinterpretation, and/or misapplication of the DOE Safety and Security Reform Plan, dated March 16, 2010, resulted in a weakened Federal security assessment program. In particular, this document stated: "Security Performance: Contractors are provided the flexibility to tailor and implement security programs in light of their situation and to develop corresponding risk- and performance-based protection strategies without excessive Federal oversight or overly-prescriptive Departmental requirements." This guidance was further expanded upon and eventually articulated in NAP–21, Transformation Governance and Oversight Initiative. The belief arose that "eyes on, hands off" precluded Federal security staff from conducting performance-based assessments of contractors. As a result, most Federal assessment was based on paperwork generated by the contractor. The paperwork was voluminous and non-standard. There were no consistent business rules on how to report areas of concern. The result was a mass of paper that made it nearly impossible to discern issues.

This paper-based system of assessment, without sufficient performance verification, is inadequate for effective evaluation of security operations. Much of the "burden" of oversight is caused by excessive paperwork associated with evaluating

compliance. Large volumes of paperwork are generated each quarter in which it is nearly impossible to discern trends or significant deficiencies. This, combined with a lack of NNSA independent observation or validation of site security implementation resulted in an inability to validate the implementation of security policies or contractor performance of assigned missions.

a. The Task Force proposed an assessment model that strengthens the role of Federal security assessment within NNSA without diminishing the legitimate need for contractors to maintain their own self-assessment capabilities.

The contractor self-assessment process is the first tier in the overall assessment process. The primary audience for the contractor self-assessments should be the contractor security managers themselves, but the self-assessments should follow a consistent, program-wide format, and be made available for review at all higher levels of management. Contractors should be required to identify, report, and resolve security issues—sanctions should come when a higher level assessment uncovers problems that the contractor self-assessments fail to identify or properly address. Even when an issue is readily resolved and corrective actions are immediate, a finding should be issued and the corrective action recorded. Failure to do so inevitably hides potential negative trends. Contractor self-assessments should involve active performance testing rather than simply relying on work observation and document review—effective security performance can only be evaluated through testing.

The fundamental purpose of Federal security performance assessment is to ensure that requirements are properly implemented. Therefore, the primary Federal assessment organization should ultimately report to the Chief of Defense Nuclear Security, who is responsible for requirements. This provides independence not only from the contractors, but also from the tactical-level Federal field staff whose necessary day-to-day interaction with contractor managers and staff risks loss of objectivity. This enables the Chief of Defense Nuclear Security to better ensure effective implementation of NNSA security programs. Additionally, it provides feedback on performance to the operational and tactical levels.

These Federal security assessments should include performance testing of all critical elements. The assessors should issue clear findings which are to be tracked and closed in a program-wide corrective action management system. Federal assessors should also look closely at the contractor self-assessment process; "failures to identify" by the contractor self-assessment element should automatically rise to the level of significant findings.

The final tier of the assessment model should explicitly rely upon the services of an independent security oversight function, currently provided by HSS. NNSA should arrange for a regular process of comprehensive inspections. The oversight function should be encouraged to issue strong findings for matters of potential concern to the NNSA Administrator and the Secretary of Energy, and should routinely evaluate the performance of contractor self-assessments and the Federal assessment program.

This performance assessment model assumes a common requirements base that is employed at all levels and across the NNSA security program. While some allowance may be made for site-specific issues, the fundamental elements of this requirements base should be an appropriately integrated system of DOE policies, NNSA implementation directives, and field operational guidance. The requirements base should be reflected in approved documents such as site Safeguards and Security Plans. Specific performance requirements should be articulated in detailed performance standards and criteria supported by a commonly understood and utilized performance testing process.

Mr. ROGERS. Mr. Friedman, your report recommends that NNSA "perform periodic in-depth reviews of contractor's security performance using a risk-based approach." Does NNSA not do this now?

a. How does NNSA and DOE use risk analysis in its assessments of security?

b. Do we have a rigorous means of assessing, managing, and balancing security risks, costs, and mission needs?

Mr. FRIEDMAN. At the time of our review, there were two levels of Federal contractor security performance assessments at the Y–12 National Security Complex. These were performed by the Department's Office of Health, Safety and Security (HSS) and the NNSA Production Office (NPO).

HSS performed limited scope security assessments on a periodic basis. During the review, we did not specifically review HSS's methodology for determining what sites/areas to assess or the frequency of the assessments. However, HSS has publically acknowledged that its review regime has been limited in recent years. The Department has stated that, as a result of the Y–12 matter, a more robust security performance assessment strategy will be implemented.

NPO stated that it performed periodic reviews of the contractor's security performance using a risk-based approach. However, as part of our work at Y–12, we interviewed the NPO personnel responsible for the reviews and examined NPO's periodic assessment reports. In our opinion, the reviews could not be considered "in-depth" since they consisted mainly of reviewing contractor-prepared documentation and/or "shadowing" the contractor's self-assessments rather than conducting independent security performance testing.

a. The results of our review at Y–12, which catalogued what we described as multiple-system failures, reflects our view of the quality of risk assessment methodologies employed by NNSA/DOE, at least as they applied to that facility at that time. Beyond our published analysis, we did not specifically evaluate NNSA/DOE's use of risk analysis to plan their security assessments. Respectfully, responsible Department officials may be able to provide a complete answer to this question.

b. Our review focused on the circumstances directly pertaining to the incident at Y–12, thus we did not evaluate the overall NNSA/DOE security posture. To the extent the problems identified at Y–12 as part of our review and by other subsequent reviews reflect the status of security throughout the complex, there is reason for concern.

Mr. ROGERS. Secretary Poneman, we've heard differing opinions on how DOE and NNSA's protective forces should be structured. Do you believe federalization of the protective forces is an appropriate path forward? What are the benefits, risks, and costs of the various models for the protective forces?

Mr. PONEMAN. Federalization of the protective force was considered extensively in security reviews by Mr. Meserve, Mr. Alston and Mr. Augustine following the Y–12 security incident as well as many others over the years. DOE believes this topic is worthy of continued dialogue within the Department and with Congress, but is not prepared to offer a formal opinion at this time.

Some of the issues for further consideration include how a Federal force would integrate with on-site Management and Operating (M&O) contractor leadership, the potential for complex-wide labor disputes or strikes, and the budgetary impact on the Government.

Mr. ROGERS. Secretary Poneman, in General Alston's letter to Secretary Chu, he says "there is a perception that corporate security policy is being written from inspection results." Mr. Augustine noted in his letter that inspections and assessments inappropriately focus on compliance with standards, and not on security effectiveness or performance, concluding that "what is needed is not more inspections but better inspections." Do you agree? If so, how will DOE address this concern?

a. What is being done to make inspections more effective at assuring robust security performance?

Mr. PONEMAN. The Department appreciates receiving these observations from General Alston and Mr. Augustine. Inspections of nuclear facilities performed by HSS not only focus on compliance with established DOE policies, but also on security effectiveness and emphasize testing of performance. I agree that the quality of inspections is very important in addition to frequency. Since the Y–12 security incident we have directed HSS to enhance its inspections to include more limited-notice and no-notice testing of the protective forces and security systems in order to ensure their readiness to respond to security incidents. As you know, we have also directed HSS to conduct extent-of-condition reviews at all Category I special nuclear facilities and to complete comprehensive inspections at each of these facilities by October 2013.

Mr. ROGERS. Secretary Poneman, several witnesses from the first panel indicated in their reports that the governance reforms initiated by Secretary Chu and Administrator D'Agostino were misinterpreted or misapplied by Federal staff, which was a contributing factor to the Y–12 incident. Do you agree? [Question #16, for cross-reference.]

Mr. PONEMAN. NNSA's governance reforms were structured to improve the Line Oversight of its contractor operations. Effective Line Oversight uses several different sources of information to ensure accurate and objective understanding of conditions and performance. Those sources include federal line management assessments, federal independent assessment and data from the Contractor's "Contractor Assurance System (CAS)". A CAS is a primary tool used by Contractor Management to measure, improve, and demonstrate performance and ensure that mission objectives and contract requirements are achieved. CAS is the same as basic concepts of successful industry quality management systems such as International Standards Organization (ISO) 9000/9001.

A robust and effectively functioning CAS provides transparency and builds trust between NNSA and its contractors and helps to ensure alignment across the NNSA Enterprise to accomplish and address mission needs. For example, comparing data

developed through the CAS to data developed by federal assessments allows NNSA to ensure that the M&O contractor has effective quality management programs in place. With effective and transparent contractor assurance systems, NNSA can focus the deployment of our federal oversight workforce on high risk areas, e.g. nuclear safety, security, and cyber security.

NNSA has recently completed a review of the current policy on reviewing CAS and Line Oversight processes in light of the lessons learned from the early reviews and the Y–12 performance failure. The review has identified needed changes to the processes so future reviews will ensure performance requirements are being met and that the objectives and expectations for NNSA governance are effectively communicated and adhered to across the complex.

These changes will be consistent with the revised DOE Order 226.1B, Implementation of Department of Energy Oversight Policy, which requires that the Heads of the Field Elements approve the initial contractor assurance system description; review and assess the effectiveness of the Contractor Assurance Systems (CAS); and establish performance expectations and communicate same to contractors through formal contract mechanisms. This is a continuation of the requirements contained in the predecessor DOE order 226.1A, dated July 31, 2007. That order also contains contractor requirements for a CAS. Additionally, DOE Order 227.1, Independent Oversight Program, issued August 30, 2011, requires that the contractor's corrective action to address a security weaknesses identified during an Independent Oversight inspection be approved by the DOE. This is a continuation of the requirement that was contained in the predecessor order, DOE Order 470.2B, Independent Oversight and Performance Assurance Program, dated October 31, 2002. A key aspect of our strengthened process is the establishment of a central line organization, the Office of Infrastructure and Operations, (NA–00) and a clear focus on oversight at three distinct, but mutually supportive, levels within NNSA. As before, the M&O contractors are responsible and accountable for their performance at the floor level where their employees perform work—this is what we call the "tactical" level of oversight. The Office of Infrastructure and Operation provides the federal line-management or "operational" oversight. In this regard, NA–00 leverages the combined capabilities of its offices through the complex to ensure that oversight is performed by both the federal staff closest to, and most knowledgeable of, a specific site's operations but also federal personnel responsible for similar activities at other locations who can provide additional objectivity because they have relevant experience but a different perspective. NNSA also provides oversight by subject matter experts who are independent of the NN–00 line organization. Offices such as security (NA–70) and safety (NA–SH) provide strategic oversight and performance data to the most senior NNSA leaders from a perspective outside the pressures and influences that can affect the line organization.

Based on these refinements and improved clarity, as well as the added reliability of the structured levels of oversight, NNSA will work to ensure that our oversight and performance expectations are clear, well executed, and not misinterpreted.

Mr. ROGERS. Secretary Poneman, DOE's 2010 Safety and Security Reform Plan advocated for a performance-focus and the removal of "excessive" Federal oversight. Do you still stand behind the plan's core tenets?

a. As Deputy Secretary, how will you ensure that NNSA and DOE conduct rigorous and effective—but not burdensome—oversight of security at NNSA's facilities?

Mr. PONEMAN. Over the past two years the Department undertook an effort to assess the effectiveness of all safety and security directives with the goal of reducing redundancy, duplication and inconsistencies. The result is a set of directives that is more streamlined, allows DOE program offices and contractors greater flexibility in implementing Departmental requirements, without sacrificing the level of protection of worker health, safety and security. The directives reform effort was not a contributing factor to the security failure at Y–12. None of the studies conducted so far (either by General Alston, Mr. Meserve, Mr. Augustine, General Finan, or the Inspector General) have pointed to the Department's revised directives. For instance, the revised DOE Order 226.1B, Implementation of Department of Energy Oversight Policy, requires that the Heads of the Field Elements approve the initial contractor assurance system description; review and assess the effectiveness of the Contractor Assurance Systems (CAS); and establish performance expectations and communicate same to contractors through formal contract mechanisms. The order also contains contractor requirements for a CAS. This is a continuation of the requirements contained in the predecessor DOE order 226.1A, dated July 31, 2007.

a. We will continue to ensure that NNSA and DOE perform rigorous and effective oversight of security and strive to improve that oversight, in ways that minimize the impact to mission execution.

Mr. ROGERS. Secretary Poneman, nearly every external review in the past decade has indicated serious problems with the security culture at NNSA and DOE. Culture changes are extremely difficult and often take a long time. What immediate-term actions should we be taking to begin this needed culture shift? What is your long-term plan to instill a new security culture? [Question #18, for cross-reference.]

Mr. PONEMAN. a. We recognize the need for a positive culture change. Immediate-term actions within the NNSA included the hiring of four senior Federal personnel to transform our approach to security. A highly-experienced individual with over 30 years of Nuclear Security experience in the Department of Defense was appointed to serve as the new Chief of Defense Nuclear Security; two new Senior Advisors experienced in security matters will serve under the Chief to develop overall policy and ensure the adequacy of its implementation through assessments. In addition, a highly experienced individual was brought into NA–00, the Office of Infrastructure and Operations, to provide high level operational experience to facilitate more consistent and high quality oversight of the operational security program. These individuals are charged with changing the culture of the security community.

Recognizing a need to continue improvement in the NNSA Safety Culture, the NNSA Administrator established the NNSA's Safety Culture Working Group (SCWG) on December 3, 2012, to identify and direct specific actions to improve the safety culture in NNSA. The SCWG quickly determined that it was appropriate, and more descriptive, to address the overall NNSA performance culture, which includes security performance. Everyone within the NNSA directly impacts our performance culture, regardless of role or function; therefore, everyone has a role in improving our overall performance culture.

The SCWG is conducting a comprehensive assessment of the NNSA culture, will analyze the data collected through extensive reviews of NNSA personnel and recommend corrective actions. The SCWG has authority to direct actions necessary to monitor and improve culture throughout NNSA.

As indicated in Geral Finan's review, after HSS security inspections revealed security flaws dating back to the early 200s, these flaws are now getting HSS follow-up attention. We recognize that true lasting cultural change is the hardest type of change to implement. NNSA senior leadership is united and engaged not only in acknowledging the need for change but in actively supporting that change. The lessons learned the hard way from our experience at Y–12 have served as an undeniable wake up call for us to set clear expectations for performance, adherence to standards and attention to detail across the NNSA enterprise.

b. First and foremost, we acknowledge the need to improve and to face facts about performance and culture head on. Our near-term actions set the stage for success in the long term. By bringing in several high quality experts with significant experience in nuclear weapons security we have begun to set the example of supreme professionalism in our leadership. We have implemented all recommendations of the Finan Report which, over time, will drive clarity not only into the chain of command but into the overall process by which we establish expectations across the enterprise.

The new assessment model implemented by NA–70, our Chief of Defense Nuclear Security organization, will drive consistency of implementation in requirements and ensure adherence to high standards across the NNSA enterprise through frequent and detailed formal assessments at our sites by independent internal NNSA security professionals.

These actions, supported by strong central leadership and unflinching focus will serve to increase the professionalism of the NNSA Headquarters security professionals, make more information available to the Administrator and hit the culture of complacency that led to our Y–12 failure directly.

Mr. ROGERS. Secretary Poneman, the first witness panel pointed out that most of their findings and recommendations are not new—that they are strikingly similar to those made by many external reviews over the past decades. We have stacks and stacks of reports going back 15 or 20 years—since before NNSA was created—describing the same exact problems. [Question #19, for cross-reference.]

a. Please list the various external reports and reviews of security and general management/oversight problems at DOE and NNSA that you have used (and will use) to understand the problems and history behind them.

b. Why are these long-standing, well-documented problems not getting fixed?

c. What assurances can you provide that they are now getting fixed? How will we know they are effective?

d. Will the Obama Administration come forward with a package of reforms that will finally address the root causes of these problems in both security and general management at DOE?

Mr. PONEMAN. In addition to the external security reviews by Mr. Meserve, Mr. Alston and Mr. Augustine and General Finan review of NNSA security following the Y–12 incident, a number of external reports and reviews of DOE/NNSA security and general management/oversight since NNSA's creation. They included:

1) Federal Advisory Committee for the Nuclear Command and Control System Comprehensive Review (Admiral Mies Report), December 3, 2009

2) Strengthening NNSA Security Expertise, an Independent Analysis (Chiles Report), March 2004

3) Science and Security in the Twenty First Centure: A Report for the Secretary of Energy on the Department of Energy Laboratories (Hamre Report), February 2002

4) Science and Security in the Service of the Nation: A Review of the Security (Baker/Hamilton Report), September 2000

The Department takes the recommendations of internal and external security experts seriously, and implements their findings and recommendations as appropriate to address systemic problems. A top priority for the Department is improving the management and oversight of the Department's nuclear security mission.

As evidenced by the Y–12 security breach, there are existing challenges in the nuclear security complex that needed to be addressed, some that demonstrated the need for a deep cultural change. Many of the external reports commented about the organization and management weaknesses, such as a lack of clear accountability, roles and responsibility, and authority. NNSA has taken on the challenge stemming from the proper line management security by implementing a key recommendation in General Finan's review, making the security of the entire nuclear complex more secure and streamlined.

Prior to the Y–12 incursion, the Headquarters NNSA security organization, the Office of Defense Nuclear Security (NA–70), served as a "Functional Manager" for the security mission, while the line authority flowed from the Secretary to other NNSA Administrators and other organizations. General Finan recommended for strategic-level policy guidance, requirements determination, and performance assessment to be under the jurisdiction of the Chief, Defense Nuclear Security (NA–70).

A separate office, NNSA' s Office of the Associate Administrator for Infrastructure and Operations (NA–00) would then provide the operational accountability for NNSA's security organization. Operational implementation and standardization of operations across the security program occurs at the NA–00 level.

The existence of a single point through which the field reports and is held accountable is the way the NNSA will assure the consistent and effective implementation of security policy. This is a change from the approach the NNSA has takenwhere each field office had greater latitude in implementing policies and requirements for its site.

Mr. ROGERS. Secretary Poneman, in his letter to Secretary Chu, Dr. Meserve notes that he and his fellow reviewers "had some difficulty in obtaining a clear organization chart that defines the structure for security oversight within DOE." He noted that issues within this problem within NNSA were going to be addressed by General Finan's effort, but that "a broader examination of DOE's internal management of security should be undertaken in order to streamline and simplify the structure." Are you going to undertake this effort to streamline and simplify DOE's management structure for security? What steps will you take and when? What can Congress do to support these efforts?

a. Are the recommendations made by General Finan on simplifying structure within NNSA being implemented?

b. How is creation of a new office that will have security responsibilities (NA–00), while maintaining or increasing the size of other offices with security responsibilities, "simplifying" the structure?

c. Will you clarify and document the roles and authorities of NA–70, NA–00, DOE's Office of Health, Safety, and Security, site offices, senior officials, and other parties? When will this happen? How will it be documented and communicated to all stakeholders?

d. What steps are you taking to minimize conflicting policies and directions provided by NNSA headquarters, DOE's Office of Health, Safety, and Security, and other Federal officials to field staff and contractors?

Mr. PONEMAN. a. NNSA is implementing recommendations made by General Finan following her thorough review of the federal NNSA security organizational structure and security oversight model.

b. General Finan offered recommendations to established and ensure a clear and strong path of line management authority, responsibility, and accountability for security operations within the NNSA. NNSA's Office of the Associate Administrator

for Infrastructure and Operations (NA–00) would provide the operational accountability for NNSA's security organization, while the Chief, Defense Nuclear Security (NA–70) provides strategic-level policy guidance, requirements determination, and performance assessment.

c. The Department's Office of Health, Safety and Security (HSS), in consultation with line management, is responsible for the development of DOE nuclear safety and security policy, Federal Rules, Orders, and the associated standards and guidance, as well as for reviewing safety and security issues complex-wide. HSS also conducts independent oversight and regulatory enforcement that is independent from line management. HSS oversight has expanded the scope and variety of performance testing methods utilized to assess the readiness of DOE and NNSA site protection systems against a defined spectrum of threats and adversary capabilities Performance testing methodologies include no-notice and limited notice inspections to obtain a more realistic assessment of site response capabilities and readiness performance.

d. To directly address problems with the assessment model, NNSA has set about implementing a three-tiered approach to assessing security throughout the NNSA. This approach includes: 1) an initial assessment performed by the contractor at the site, 2) an assessment of the contractor's performance carried out by the Chief of Defense Nuclear Security at DOE Headquarters (NA–70), and 3) independent oversight by the Office of Health, Safety and Security. And, of course, apart from this three-tiered assessment and inspection regimen, we expect Federal site personnel to perform quality assurance activities on a routine basis as an integral part of their line management responsibilities.

Mr. ROGERS. Secretary Poneman, in the 1990s we had a string of major security problems at DOE Defense Programs, which then ran the nuclear weapons complex. In 1999, the President's Foreign Intelligence Advisory Board called DOE "security at its worst" and a "dysfunctional bureaucracy that has proven it is incapable of reforming itself." Congress created NNSA in an effort to address these exact concerns. But on February 22 the DOE Chief Security Officer, Glenn Podonsky, was quoted telling a reporter that the nuclear enterprise "wasn't working badly" in the 1990s before NNSA was formed, and that we should just abolish NNSA and go back to having everything in DOE.

a. Do you agree with Mr. Podonsky that the nuclear enterprise "wasn't working badly" in the 1990s?

b. Do you agree with Mr. Podonsky that NNSA should be dissolved and folded back into DOE? Are Mr. Podonsky's views the position of the Department of Energy?

Mr. PONEMAN. I discussed Mr. Podonsky's remarks with him. His comments were not accurately reflected in the news article you are referencing, and he made clear at the time that the remarks were not made on behalf of DOE. He merely remarked on the restructuring options that an external review panel may consider and the feasibility of those options. As you know, the Administration has made no proposal to dissolve the NNSA or to return to any previous organizational model.

Mr. ROGERS. Secretary Poneman, are you aware that DOE's Office of Health, Safety, and Security conducted an independent oversight inspection of Y–12's physical security systems in May 2012—just two months before the security breach?

a. When did you become aware of this inspection and its results?

b. Do you believe this inspection of Y–12's physical security systems should have found the many problems—such as inoperative cameras, unacceptably high false alarm rates, inappropriate delegation of cognizant security authority, etc.—that were subsequently found to have contributed to the breach?

c. How effective are these independent inspections if they can't catch and correct these glaring problems?

Mr. PONEMAN. The report from May 2012 was not a full security inspection, nor was this report approved through the formal HSS review process. Official HSS reports go through an exhaustive peer-review process led by a Quality Review Board and are approved by all levels of HSS senior management including approval by the Chief Health, Safety and Security Officer. The May 2012 report was never considered by a Quality Review Board panel and was not reviewed or approved by HSS senior management. The individual who wrote it and submitted it to the site, (without a signature nor on DOE letterhead) has received a formal reprimand for his misrepresentation and was removed from any leadership role for failing to follow important protocols and misrepresenting the nature of the product.

A security inspection by HSS would have revealed many of the problems at Y–12—as did the most recent full inspection in 2008–2009. This unsanctioned report was the product of an assistance visit requested by the site to focus on some very narrow issues. This unapproved memo in no way could be interpreted as a valida-

tion that everything was OK with security at Y–12. Neither HSS senior management nor I were aware of the document until it was identified during a search for Y–12 related documents requested by Congress.

Mr. ROGERS. Secretary Poneman, how long has DOE's Chief Security Officer, Mr. Glenn Podonsky, been employed by the Department of Energy? How long has he held senior positions in the Department that have to do with security oversight and/or security policy?

a. Given his previous positions and tenure, do you believe Mr. Podonsky should have been aware of external reviews of DOE security from the 2000s (Such as the Commission on Science and Security in 2002 and the Mies Task Force in 2005)?

b. As the Chief Security Officer for the Department, do you believe it is Mr. Podonsky's responsibility to ensure that problems identified by previous external reviews of security are corrected?

c. Do you believe the problems identified by previous reviews, such as "lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes, " as identified by Admiral Rich Mies in 2005 and many others before him, have been addressed?

Mr. PONEMAN. Mr. Podonsky has served in DOE for approximately 29 years, in a number of senior positions involving security evaluations, independent oversight, and performance assurance. He has been relied upon by DOE leaders and Congressional oversight committees through those years due to his experience and expertise in DOE nuclear security matters. It is important to understand the security role of the Office of Health, Safety and Security (HSS) which is headed by Mr. Podonsky. HSS is a staff office reporting directly to me and the Secretary. HSS leads the development of Departmental security policies, and provides us with unvarnished assessments of DOE program and facility security performance. Those assessments are performed independently of the line management which holds responsibility for managing security at our sites and facilities. However because HSS is independent of line management within the programs, it does not have authority to direct the Federal or contractor security officials at each site; it is up to these parties to take actions in response to HSS findings. HSS ideally plays a role in helping the programs implement security recommendations, and follow-up to ensure that those recommendations are adequately addressed. Over his career Mr. Podonsky has been well aware of the various internal and external studies that have been done on DOE security, and he has been involved at a senior level alongside previous Secretaries and Deputy Secretaries and the DOE program office line management, in determining the most appropriate response to each study.

Mr. ROGERS. Secretary Poneman, do you still have confidence in Mr. Podonsky as the Department's Chief Security Officer? Do you intend to hold him or his office accountable for failing to identify the myriad security problems at Y–12 just two months prior to the incident, or for failing to correct the long-standing security problems at DOE?

Mr. PONEMAN. We see HSS as an important source of the solution. All of us in the DOE security community—from the Secretary and me to program office and site management in both headquarters and the field, including HSS, have an obligation to improve security performance and we are taking bold steps to ensure that the special nuclear materials of the DOE are adequately protected. For all of us who have not been removed from the line management of security following the incident, it is our sole duty to ensure that we have learned from the incident and quickly and effectively implemented corrective actions. HSS has been a key contributor to that effort. Since the Y–12 incident, HSS has led a successful extent-of-condition review of all DOE facilities which hold Category I special nuclear materials, and is now in the process of executing exhaustive inspections at each of these sites, to include enhanced force-on- force testing of our protective forces, as directed by the Secretary.

Mr. ROGERS. Administrator Miller, all of the studies the committee is aware have been conducted after the Y–12 incident have been finalized except the "Special Review Team" report conducted by NA–70. Initially, the committee was told that this assessment was expected to "contribute to the wider effort to identify root causes, develop conclusions, and outline recommendations" for security improvements at Y–12 and in other agency facilities. However, although the team's work apparently concluded in September, it's been five months and the report has not yet been finalized. What is the reason for this delay?

a. Have NNSA and DOE decided to discount the review because it was conducted by an organization whose oversight practices contributed to the incident? If that's the case, then why was the HSS review not similarly discounted, given that HSS gave the physical security system at Y–12 a clean bill of health just two months

prior to the incident? Or is it that senior NNSA or DOE officials disagree with the recommendations and conclusions that the SRT report draws?

Ms. MILLER. As soon as the Special Review Team (SRT) returned from Tennessee, they shared their insights and findings with the Chief, Defense Nuclear Security (CDNS) who took immediate action to resolve the issues cited. One of his actions was the immediate sharing of lessons learned with field offices as well as the five page summary of the issues found at Y–12 for use in assessing and improving their processes. That summary was also provided to the House Armed Services Committee. Additionally, in January 2013, a draft version of the Y–12 Special Review Team report was provided to the House Armed Services Committee; however, the "Assessment of NNSA Federal Organization and Oversight of Security Operations" study was well underway and was yielding important recommendations. That report has since been completed and published, and was provided to the House Armed Services Committee staffers in December 2012.

a. We value the information provided in the SRT report, and many of their observations focused on the larger National Nuclear Security Administration security program, and are applicable to all of our operations. It is also important to note that the May 2012 HSS Site Assistance Visit report that you cite as giving the physical security system at Y–12 "a clean bill of health," did not represent a full security inspection of Y–12, but only examined a few site specific issues HSS was asked to help assess.

Mr. ROGERS. Administrator Miller, how is NNSA handling the conflicting recommendations generated from the various post-Y–12 incident studies? For instance, the DOE–HSS and Finan reports recommend conducting more hands-on oversight of security, while Mr. Augustine and two external members of the SRT panel caution specifically against this. [Question #22, for cross-reference.]

a. As the Acting Administrator, how will you ensure that NNSA and DOE conduct rigorous and effective—but not burdensome—oversight of security at NNSA's facilities?

Ms. MILLER. NNSA leadership implemented several processes and procedures to improve security throughout the enterprise and ensure a consistent standard for security operations. The Office of Defense Nuclear Security (NA–70) has been realigned to focus on policy development, strategic planning, and independent performance assessments of security activities. The Office of Infrastructure and Operations (NA–00), comprised of the NNSA Field Offices will develop an internal performance review culture that will supplement the local field offices. These performance reviews will be staffed by field office employees from other sites and be specifically integrated with other audit and surveillance plans to minimize operational impacts. To elaborate, I have revised our processes so that NNSA will rely on a three-tiered assessment model that will focus on performance and outcomes (not just process) at the tactical, operational, and strategic levels. The contractor self-assessment process continues as a "tactical level" first tier in the overall assessment process. The Office of Infrastructure and Operations, drawing on NNSA federal resources from across the complex, will provide "operational level" oversight to ensure consistent and effective performance from a line management perspective. Finally, the "strategic" oversight is conducted by NA–70/CDNS. An internal independent Federal assessment organization, which reports directly to the Chief of Defense Nuclear Security, and will ensure requirements are properly implemented by going to the field, with minimal notice, and assessing security readiness, operations, and implementation. A final tier of the assessment model completely separate from NNSA is currently provided by the Office of Health, Safety and Security.

a. As described in the response to Q22 [above], NNSA will employ a system of tactical, operational, and strategic oversight.

Mr. ROGERS. Administrator Miller, we've heard differing opinions on how DOE and NNSA's protective forces should be structured. Do you believe federalization of the protective forces is an appropriate path forward? What are the benefits, risks, and costs of the various models for the protective forces?

Ms. MILLER. I defer to the Deputy Secretary of Energy's response. [See page 131.]

Mr. ROGERS. Acting Administrator Miller, do you believe NNSA has a rigorous means of assessing, managing, and balancing security risks, costs, and mission needs? If so, please describe this process.

Ms. MILLER. Yes I do. NNSA leadership has implemented several processes and procedures to improve security throughout the enterprise and ensure a consistent standard for security operations.

We realigned security resource execution to the Office of Infrastructure and Operations (NA–00) in alignment with its operational authority across all NNSA sites.

- NA–00 is assuming operational control over security implementation across the Nuclear Security Enterprise.

- Specifically, NA–00 will ensure:
  - standardization of security procedures across the field locations;
  - provide operational assistance; and
  - serve as a conduit for operational concerns to the DNS staff.

Additionally, the Defense Nuclear Security (DNS) mission was reinvigorated to focus on policy development, strategic planning, and performance assessments of field-led activities.

For example, as NNSA Acting Administrator, I recently dispatched the new Acting Chief of DNS, travelling with a team of security professionals, to visit every NNSA site during his first 50 days in office, executing limited and no-notice assessments of their security readiness, operations, and program implementation. These site visits are the first step in what will become an enduring mission focus. NNSA is committed to change our culture of how we assess security so that we are less reliant on reports written by others and more focused on our own real time assessments with a "boots on-the-ground" approach.

Mr. ROGERS. Acting Administrator Miller, how much has the response and aftermath to the Y–12 incident cost? How is NNSA paying for these costs? Do you expect security costs to increase dramatically at Y–12 and/or across the enterprise in Fiscal Year 2014 and beyond?

Ms. MILLER. The costs incurred for immediate corrective actions in FY 2012 were approximately $13,680K. Approximately $2,984K of this amount were indirect costs funded from organizational overhead pools. Approximately $10,696K were paid for directly from the Field Security (FS–20) account, but managed within the funding already allocated to the site prior to the event. Total costs will depend on NNSA approval of the specific baseline increases and non- recurring project/procurements proposed by the site. For FY13 and beyond, these are still being carefully vetted by subject matter experts and senior decision makers and will be subject to the results of a new vulnerability analysis. DNS expects there may be some minor increases in the recurring level of effort, but most corrective actions have been and will be largely one-time costs.

Mr. ROGERS. Administrator Miller, several witnesses from the first panel indicated in their reports that the governance reforms initiated by Secretary Chu and Administrator D'Agostino were misinterpreted or misapplied by Federal staff, which was a contributing factor to the Y–12 incident. Do you agree?

Ms. MILLER. Please see the answer the Deputy Secretary gave in response to question #16. [See page 131.]

Mr. ROGERS. Administrator Miller, NNSA has created the "NA–00" organization to manage the site offices. It will also have a role in overseeing security at NNSA facilities. How will this new organization fit into the many other organizations with security responsibilities, including NA–70, DOE–HSS, and the site offices? Are you confident that this extra office will resolve these long-standing problems with security organization, policy, and oversight? Are you at all concerned that this additional office will simply complicate an already too-complicated structure?

Ms. MILLER. First and foremost, it is important to clarify that NA–00 is not actually an additional layer or office. It is the combination of all NNSA Site Offices into a single operational entity. So, rather than have eight independent operational level entities, each establishing standards and procedures and setting expectations locally, the NA–00 organization will fulfill those functions on an enterprise basis. The Office of Infrastructure and Operations (NA–00), with enterprise operational responsibilities will drive consistent implementation of requirements across the Nuclear Security Enterprise.

Specifically, NA–00 will:

- ensure consistent implementation of security policies while allowing for purposeful differences;
- deliver high quality engaged and active oversight of security operations;
- provide operational assistance between field offices; and
- serve as a conduit for operational concerns to the Defense Nuclear Security staff.

Establishment of NA–00 will allow the Office of Defense Nuclear Security (NA–70) to focus on policy development, strategic planning, and perform independent assessments of security activities. Yes, I am confident that this new organization structure will resolve the long-standing problems with security organization, policy, and oversight

No, I do not believe this new organizational structure will cause any confusion. These organizational changes will result in clearer roles, responsibilities, and authorities.

Mr. ROGERS. Acting Administrator Miller, nearly every external review in the past decade has indicated serious problems with the security culture at NNSA and DOE.

Culture changes are extremely difficult and often take a long time-what immediate-term actions should we be taking to begin this needed culture shift? What is your long-term plan to instill a new security culture? What is your plan to attract the kinds of experts and knowledge-base that are needed to perform effective oversight?

Ms. MILLER. Please see the Deputy Secretary's answer to question #18. [See page 133.]

---

## QUESTIONS SUBMITTED BY MR. COOPER

Mr. COOPER. General Alston, do NNSA contractors have too little independent oversight, or too much?

General ALSTON. There was poor quality oversight of the contractor providing security at Y–12. The "eyes on, hands off" signal from the HQ, together with insufficient and inadequate performance-based assessments contributed to poor oversight conditions. Other sites' security operations, however, performed satisfactorily, in spite of 'hands off' atmospherics. The quality of the oversight is one several key ingredients to effective performance.

Mr. COOPER. Do you believe that the incident is the result of overly burdensome security requirements, as some have claimed?

General ALSTON. I saw no evidence to substantiate overly burdensome security requirements as causal or even contributing to the incident. The NNSA "eyes on, hands off" signal contributed to a lack of sufficient oversight that empowered too much local discretion at Y12 that resulted in additional and unjustifiable mission risk.

Mr. COOPER. What should be done at the contract level to increase accountability and liability for failures? Should the government be able to seek damages for non-performance? Should criminal liability be an option?

General ALSTON. I don't feel qualified to comment on or suggest specific contracting options to ensure proper security performance because the duration of the project was short and the direction from the Secretary of Energy did not lead me in that direction. I personally wouldn't prefer to secure nuclear materials with contractors. But if DOE and NNSA continue to purchase protective services, governance requirements and accountability needs to be squared away with the government overseers first.

Mr. COOPER. General Finan, do you think that NNSA has gone too far in delegating responsibility for making security decisions to its contractors?

General FINAN. Yes, in some cases. There was no clear policy guidance on what could be delegated or how the delegations would be implemented. NAP- 70.2, Physical Protection, has allowed for varied interpretations of what can and cannot be delegated. There was no standardized process for the delegation of CSA from the Chief of Defense Nuclear Security to the Federal security managers. Further delegation of CSA to the security contractor was inconsistently exercised and in some cases inappropriate. As a result, the contractor was sometimes allowed to approve security plans and procedures without effective Federal oversight or approval.

Mr. COOPER. General Finan, do NNSA contractors have too little independent oversight, or too much?

General FINAN. NNSA contractors do not have the right kind of oversight. Much of the "burden" of oversight is caused by excessive paperwork associated with evaluating compliance. The current security assessment process in NNSA is paper-based and is heavily dependent on field office and contractor reporting. Large volumes of paperwork are generated each quarter in which it is nearly impossible to discern trends or significant deficiencies.

In the area of security, oversight must be about performance. Therefore, oversight should see actual performance in the form of real world activity or exercises. Some paperwork should be reviewed, such as training records, but that paper work should already exist and not be generated solely for the purpose of outside oversight. Specific standards against which security operations are to perform and the criteria by which they will be evaluated must be codified. This will ensure security contractors know what is expected and how they will be evaluated. By eliminating paperwork generated solely for the purpose of oversight and adhering to a known set of standards and criteria, security oversight should not be burdensome.

Mr. COOPER. Do you believe that the incident is the result of overly burdensome security requirements, as some have claimed?

General FINAN. No. A lack of clearly defined security requirements contributed to the incident. There is no clearly established requirements-driven baseline to govern the implementation of the NNSA security program. Rather, the NA–70 approach deliberately departed from key DOE Security Orders and established a less restrictive

security policy framework through the NAPs without resolving the different performance measurement expectations between the two policies. The lack of clearly defined performance requirements resulted in inconsistent and incomplete security program implementation. A performance baseline, set forth in detailed standards and criteria, is the keystone of an effective security program. Precisely articulated standards and criteria further provide an objective foundation for performance assessment. Currently, NNSA does not have the standards or criteria necessary to effectively measure security program performance. The Task Force noted that the lack of standards and criteria has been coupled with the widespread notion that contractors must only be told "what" the mission is, not "how" the mission is to be accomplished. Therefore, security tasks are not necessarily performed in a manner consistent with NNSA security requirements.

We should also resist the notion that strong performance-based standards and criteria and an equally strong insistence on stringent performance assessment and oversight inherently constitutes an excessive burden on contractors and the field. Part of the cultural challenge lies in overcoming the tendency on the part of contractors and their field level federal counterparts to assert that their local priorities and perspectives must take precedence over comprehensive and coherent, centrally-driven security program direction. A good system must take into account special local circumstances. However, NNSA's longstanding tradition has been the assertion that "the field always knows best," and that Headquarters should simply stay out of their business. Upon close examination, many complaints about "excessively burdensome HQ security oversight" are revealed as exercises in "turf protection".

Mr. COOPER. What should be done at the contract level to increase accountability and liability for failures? Should the government be able to seek damages for nonperformance? Should criminal liability be an option?

General FINAN. This is largely an issue for contracting. It is important that responsibilities and authorities are properly aligned. Each organization needs to have clearly defined responsibilities. With each of these responsibilities, the appropriate authority must be accorded. With responsibility and authority in alignment, individual and organizational accountability is established.

Mr. COOPER. Mr. Friedman, do you think that NNSA has gone too far in delegating responsibility for making security decisions to its contractors?

Mr. FRIEDMAN. Given the structure of NNSA (specifically, the number of contractor versus Federal personnel), extensive responsibility for security decisions has been delegated to contractors. This having been said, we found that Federal oversight of the contractors and their security decisions was inadequate. At Y–12 the lack of local Federal involvement in technical security issues and NNSA's "eyes on, hands off" policy were troubling, suggesting to us that the relationship between contractor responsibility and Federal responsibility for site security was out of balance.

Mr. COOPER. Mr. Friedman, do NNSA contractors have too little independent oversight, or too much?

Mr. FRIEDMAN. In my opinion, NNSA contractors have too little independent oversight. Local Federal oversight had employed an "eyes on, hands off" approach, with limited independent performance testing/assessment. In recent years the number and scope of reviews by HSS has also been reduced.

Mr. COOPER. Do you believe that the incident is the result of overly burdensome security requirements, as some have claimed?

Mr. FRIEDMAN. No. Our reviews of security across the complex have not revealed examples of what we considered to be overly burdensome security requirements. Rather, we found that the incident at Y–12 resulted from multiple system failures on several levels. For example, we identified troubling displays of ineptitude in responding to alarms, failures to maintain critical security equipment, over-reliance on compensatory measures, misunderstanding of security protocols, poor communications, and weaknesses in contract and resource management. So-called burdensome security requirements were not part of the sequence of events at Y–12.

Mr. COOPER. What should be done at the contract level to increase accountability and liability for failures? Should the government be able to seek damages for nonperformance? Should criminal liability be an option?

Mr. FRIEDMAN. To increase accountability and liability for failures at the contract level, performance measures should be added to each contractor's Performance Evaluation Plan to incorporate security into each mission element. Such action would hopefully prevent contractors from earning full performance fees unless security is: (1) integrated into day-to-day processes and, (2) found to be effective and efficient by external reviewers. While the fee structure provides an incentive for excellence in contractor performance in the security arena, the NNSA/DOE should not be reluctant to terminate contracts for poor performance. That may be an extreme meas-

ure for some, but when national security interests are at stake, it is a step which needs to be available to, and exercised by, Federal managers.

Mr. COOPER. Secretary Poneman, are lessons from the deficiencies in security oversight being applied to safety oversight? How?

Mr. PONEMAN. Yes. Where we see opportunities for improvement identified in our response to the Y–12 security incident which can also be employed to improve our oversight of safety, we will seek to do so. A fundamental failure in the Y–12 incident was the inadequate flow of information about underlying security problems up through the management chain. Under the leadership of the Office of Health, Safety and Security (HSS), over the past year a number of independent assessments have identified deficiencies in safety culture at several DOE projects, sites and programs. We know now that we must do a better job in creating an environment where employees at all levels feel motivated to identify deficiencies in both safety and security, and feel confident that they can bring those problems forward without retaliation and to work with management to develop appropriate solutions. This, too, is a very high priority for our leadership team.

Mr. COOPER. Secretary Poneman, what was the cost of overtime to avoid delays due to Y–12 being shut down?

Mr. PONEMAN. Following the security incident in July 2012, operations activities at Y–12 were shut down from July 30 to August 14, 2012, for a total of 10 days. This shutdown impacted a number of operations activities, including Category 1 and 2 Special Nuclear Materials Operations. Restart of these activities were phased back in on August 15, 2012; overtime costs of about $34,000 were incurred in order to get the work back on schedule.

Mr. COOPER. Secretary Poneman, B&W got nearly 60% of its award fee in FY2012. The security failure at Y–12 only cost them $12 million in un-earned fee. [Question #42, for cross-reference.]

- What should be done at the contract level to increase accountability and liability for failures? Should the government be able to seek damages for non-performance and be able to impose fines?
- Should criminal liability be an option to improve the incentives for performance and the contractor culture?
- Other than docking Babcock & Wilcox's award fee for security, is NNSA attempting to get back part of the more than $150 million that was spent on security, given non performance?

Mr. PONEMAN. The contract, along with existing Federal and DOE Acquisition Regulations, have sufficient terms and conditions to hold contractors accountable and liable for performance failures. Additionally, given the unprecedented nature of this failure, the Department is reviewing our existing regulatory authorities to determine if these need to be expanded to cover the security of special nuclear materials.

The Department possesses statutory and regulatory authority to impose civil penalties. In addition, I believe adequate and sufficient criminal laws are already in place. Federal criminal law involving fraud, conflict of interest, bribery or gratuity violations and false claims are currently applicable, as appropriate, to contractors. In addition, contractors must ensure that no false, fictitious, or fraudulent statements are made to a Federal agency under 18 U.S.C. § 1001.

The Department is in the process of reviewing the matter and will enforce its rights under the contract to hold Babcock & Wilcox Y12 accountable for its deficient work, including withholding payment of costs if appropriate.

Mr. COOPER. Secretary Poneman, nearly every external review in the past decade has indicated serious problems with the security culture at NNSA and DOE. Culture changes are extremely difficult and often take a long time—what immediate-term actions should we be taking to begin this needed culture shift?

- What is your long-term plan to instill a new security culture?
- What is your plan to attract the kinds of experts and knowledge-base that are needed to perform effective oversight?

Mr. PONEMAN. Please see Deputy Secretary Poneman's response to question 18 for an answer to the first bullet. [See page 133.] The answer to the second bullet is provided by Deputy Secretary Poneman's response to question 19. [See pages 133–134.]

Mr. COOPER. Secretary Poneman, how are you ensuring that Federal oversight performs site vulnerability analyses that look at the systemic impact and the broader implications of individual security decisions? [Question #46, for cross-reference.]

Mr. PONEMAN. The current vulnerability analysis (VA) process is driven at the site level. While this ensures results that are highly tailored to individual site-specific parameters, it can also produce widely divergent approaches to security across the NNSA.

This issue was recognized in General Finan's Report "Assessment of NNSA Federal Organization and Oversight of Security Operations." The report was the main driver for the establishment of the Office of Security Operations (NA–00–30) within the larger NA–00 Office of the Associate Administrator for Infrastructure and Operations. Consistent with the recommendations of the Finan Report, NA–00–30 will be the centralized security function for NNSA that ensures line management authority, responsibility, and accountability for the security program within the NNSA.

In its role as the centralized security function, NA–00–30 will establish a new centralized VA process that employs a core team of VA experts teamed with site subject matter experts to produce site-specific analyses while gaining consistency across the Enterprise, identifying systemic issues and broader implications, and ensuring greater transparency and justification for Field Security (FS–20) budget requests.

Mr. COOPER. Acting Administrator Miller, are lessons from the deficiencies in security oversight being applied to safety oversight? How?

Ms. MILLER. Yes. Lessons learned from the Y12 security incident are being applied to safety oversight. The organizational changes and revised oversight approach for security are also being implemented for safety. In addition, NNSA is working aggressively to evaluate and improve its safety culture across all sites. Although this effort began before the Y12 event, strengthening NNSA's safety conscious work environment will help ensure contractor and Federal personnel are encouraged and motivated to identify and seek resolution of safety issues and to raise these issues up through the management chain. One of the more significant lessons learned in the Y–12 incident was that known, significant issues with security were not being raised from subject matter experts up through the NNSA management chain.

Mr. COOPER. Acting Administrator Miller, what was the cost of overtime to avoid delays due to Y–12 being shut down?

Ms. MILLER. Following the security incident in July 2012, operations activities at Y–12 were shut down from July 30 to August 14, 2012, for a total of 10 days. This shutdown impacted a number of operations activities, including Category 1 and 2 Special Nuclear Materials Operations. Restart of these activities were phased back in on August 15, 2012; overtime costs of about $34,000 were incurred in order to get the work back on schedule.

Mr. COOPER. Acting Administrator Miller, B&W got nearly 60% of its award fee in FY2012. The security failure at Y–12 only cost them $12 million in un-earned fee.

- What should be done at the contract level to increase accountability and liability for failures? Should the government be able to seek damages for non-performance and be able to impose fines?
- Should criminal liability be an option to improve the incentives for performance and the contractor culture?
- Other than docking Babcock & Wilcox's award fee for security, is NNSA attempting to get back part of the more than $150 million that was spent on security, given non-performance?

Ms. MILLER. Please see Deputy Secretary Poneman's response to question 42. [See page 141.]

Mr. COOPER. Acting Administrator Miller, nearly every external review in the past decade has indicated serious problems with the security culture at NNSA and DOE. Culture changes are extremely difficult and often take a long time—what immediate-term actions should we be taking to begin this needed culture shift?

- What is your long-term plan to instill a new security culture?
- What is your plan to attract the kinds of experts and knowledge-base that are needed to perform effective oversight?

Ms. MILLER. For response to the first part of the question on security culture, please see response to question 18. [See page 133.]

In addition to our overall efforts to improve the NNSA performance culture, we are taking additional actions to specifically address security. We have recruited new leaders for both the Office of Defense Nuclear Security (NA–70) and the office of security within the Office of Infrastructure and Operations (NA–00). Those leaders come to us from outside the Department of Energy and bring vast and varied sets of skills and experience from their careers in the Department of Defense nuclear community.

Besides the infusion of new leadership, we are encouraging a questioning attitude from the people that perform the work day-to-day at the sites. While it is easy to fall into routines that contribute to the effect of not being able to see the forest for the trees, encouraging employees to question the status quo also promotes ownership and understanding of the security processes.

Another thing we plan to incorporate into the NA–00 performance assurance process is the use of security professionals from across the complex to augment our assessments. This provides several advantages; it allows security professionals from other sites to participate in the evaluation process removing the mystique, takes advantage of and recognizes the professionals at the other sites, and encourages the sharing of best practices. All of these contribute to instilling a new security culture.

Additionally, NA–70 will focus on policy development, strategic planning, and performance assessments of field activities.

Using small assessment teams of security experts with minimal advanced notice to the sites, NA–70 will assess security readiness, operations and program implementation of both the Federal and contractor security elements. These assessments will be short in duration but repetitive throughout the year.

This new assessment approach will require additional oversight personnel. NA–70 is working to recruit additional Federal senior security specialists. These individuals will augment the current Federal senior security specialists to allow for the execution of a rigorous assessment program.

We are working with our Human Capital community in an effort to target recruitment of oversight personnel toward communities that are rich in the basic skill sets germane to the mission. Specifically, we are looking to tap into the pool of resources which have previously served an oversight and/or assessment role in support of the National nuclear security mission.

Mr. COOPER. Acting Administrator Miller, how are you ensuring that Federal oversight performs site vulnerability analyses that look at the systemic impact and the broader implications of individual security decisions?

Ms. MILLER. Please see Deputy Secretary Poneman's response to question 46. [See page 141.]

○