

NASA SECURITY: ASSESSING THE AGENCY'S EFFORTS TO PROTECT SENSITIVE INFORMATION

JOINT HEARING

BEFORE THE
SUBCOMMITTEE ON SPACE &
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRTEENTH CONGRESS
SECOND SESSION

—
JUNE 20, 2014
—

Serial No. 113–81
—

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

—
U.S. GOVERNMENT PRINTING OFFICE

89–410PDF

WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

DANA ROHRABACHER, California	EDDIE BERNICE JOHNSON, Texas
RALPH M. HALL, Texas	ZOE LOFGREN, California
F. JAMES SENSENBRENNER, JR., Wisconsin	DANIEL LIPINSKI, Illinois
FRANK D. LUCAS, Oklahoma	DONNA F. EDWARDS, Maryland
RANDY NEUGEBAUER, Texas	FREDERICA S. WILSON, Florida
MICHAEL T. McCAUL, Texas	SUZANNE BONAMICI, Oregon
PAUL C. BROUN, Georgia	ERIC SWALWELL, California
STEVEN M. PALAZZO, Mississippi	DAN MAFFEI, New York
MO BROOKS, Alabama	ALAN GRAYSON, Florida
RANDY HULTGREN, Illinois	JOSEPH KENNEDY III, Massachusetts
LARRY BUCSHON, Indiana	SCOTT PETERS, California
STEVE STOCKMAN, Texas	DEREK KILMER, Washington
BILL POSEY, Florida	AMI BERA, California
CYNTHIA LUMMIS, Wyoming	ELIZABETH ESTY, Connecticut
DAVID SCHWEIKERT, Arizona	MARC VEASEY, Texas
THOMAS MASSIE, Kentucky	JULIA BROWNLEY, California
KEVIN CRAMER, North Dakota	ROBIN KELLY, Illinois
JIM BRIDENSTINE, Oklahoma	KATHERINE CLARK, Massachusetts
RANDY WEBER, Texas	
CHRIS COLLINS, New York	
BILL JOHNSON, Ohio	

SUBCOMMITTEE ON SPACE

HON. STEVEN M. PALAZZO, Mississippi, *Chair*

RALPH M. HALL, TEXAS	DONNA F. EDWARDS, Maryland
DANA ROHRABACHER, California	SUZANNE BONAMICI, Oregon
FRANK D. LUCAS, Oklahoma	DAN MAFFEI, New York
MICHAEL T. McCAUL, Texas	JOSEPH P. KENNEDY III, Massachusetts
MO BROOKS, ALABAMA	DEREK KILMER, Washington
LARRY BUCSHON, Indiana	AMI BERA, California
STEVE STOCKMAN, Texas	MARC VEASEY, Texas
BILL POSEY, Florida	JULIA BROWNLEY, California
DAVID SCHWEIKERT, Arizona	FREDERICA WILSON, Florida
JIM BRIDENSTINE, Oklahoma	EDDIE BERNICE JOHNSON, Texas
CHRIS COLLINS, New York	
LAMAR S. SMITH, Texas	

SUBCOMMITTEE ON OVERSIGHT

HON. PAUL C. BROUN, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin	DAN MAFFEI, New York
BILL POSEY, Florida	ERIC SWALWELL, California
KEVIN CRAMER, North Dakota	SCOTT PETERS, California
BILL JOHNSON, Ohio	EDDIE BERNICE JOHNSON, Texas
LAMAR S. SMITH, Texas	

CONTENTS

June 20, 2014

Witness List	Page 2
Hearing Charter	3

Opening Statements

Statement by Representative Steven M. Palazzo, Chairman, Subcommittee on Space, Committee on Science, Space, and Technology, U.S. House of Representatives	11
Written Statement	12
Statement by Representative Dan Maffei, Ranking Minority Member, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	13
Written Statement	14
Statement by Representative Paul C. Broun, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	15
Written Statement	16
Statement by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives	17
Written Statement	17

Witnesses:

Mr. Richard Keegan, Associate Deputy Administrator, National Aeronautics and Space Administration	
Oral Statement	18
Written Statement	20
Ms. Belva Martin, Director, Acquisition and Sourcing Management, Government Accountability Office	
Oral Statement	31
Written Statement	33
Ms. Gail A. Robinson, Deputy Inspector General, National Aeronautics and Space	
Oral Statement	48
Written Statement	50
Mr. Douglas Webster, Fellow, National Academy of Public Administration and Principal, Cambio Consulting Group	
Oral Statement	57
Written Statement	59
Discussion	75

Appendix I: Answers to Post-Hearing Questions

Mr. Richard Keegan, Associate Deputy Administrator, National Aeronautics and Space Administration	90
Ms. Belva Martin, Director, Acquisition and Sourcing Management, Government Accountability Office	112
Ms. Gail A. Robinson, Deputy Inspector General, National Aeronautics and Space	119

IV

	Page
Mr. Douglas Webster, Fellow, National Academy of Public Administration and Principal, Cambio Consulting Group	126

Appendix II: Additional Material for the Record

Submitted statement for the record by Representative Donna F. Edwards, Ranking Minority Member, Subcommittee on Space, Committee on Science, Space, and Technology, U.S. House of Representatives	142
Responses submitted by NASA for information requested by Chairman Broun during the course of the hearing	144

**NASA SECURITY: ASSESSING THE AGENCY'S
EFFORTS TO PROTECT SENSITIVE
INFORMATION**

FRIDAY, JUNE 20, 2014

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEES ON SPACE &
OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:01 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Steven Palazzo [Chairman of the Subcommittee on Space] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

1321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

Subcommittee on Space
and
Subcommittee on Oversight

***NASA Security: Assessing the Agency's Efforts to Protect
Sensitive Information***

Friday, June 20, 2014
10:00 a.m. to 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

*Mr. Richard Keegan, Associate Deputy Administrator, National Aeronautics and Space
Administration*

*Ms. Belva Martin, Director, Acquisition and Sourcing Management, Government Accountability
Office*

*Ms. Gail A. Robinson, Deputy Inspector General, National Aeronautics and Space
Administration*

*Mr. Douglas Webster, Fellow, National Academy of Public Administration and Principal,
Cambio Consulting Group*

**U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Space
Subcommittee on Oversight**

NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information

CHARTER

Friday, June 20, 2014
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

The Subcommittees on Space and Oversight will hold a joint hearing, *NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information*, at 10:00 a.m. on Friday, June 20, 2014. The Government Accountability Office (GAO), the National Academy of Public Administration (NAPA), and the NASA Office of Inspector General (OIG) have all released reports within the past several months addressing how NASA manages access of NASA facilities and sensitive information to foreign nationals. This hearing will review these practices and procedures, as well as recommendations for improvement identified in these reports.

Witnesses

- **Mr. Richard Keegan**, Associate Deputy Administrator, National Aeronautics and Space Administration;
- **Ms. Belva Martin**, Director, Acquisition and Sourcing Management, Government Accountability Office;
- **Ms. Gail A. Robinson**, Deputy Inspector General, National Aeronautics and Space Administration;
- **Mr. Douglas Webster**, Fellow, National Academy of Public Administration and Principal, Cambio Consulting Group.

Background

The National Aeronautics and Space Act of 1957 directs that NASA “provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof.”¹ Conversely, the Act also directs NASA to protect classified, trade secret, and confidential information.² Additionally, NASA—like other federal agencies—is subject to the requirements of the Arms Export Control Act and the Export Administration Act.³

¹ 51 U.S.C. §20112(a)(3)

² 51 U.S.C. §20131 and 20132

³ 22 U.S.C. §2751-2799aa-2 and 50 U.S.C. app. §2401-2420

Two high-profile events highlighted this tension:

- On March 16, 2013, agents from the Department of Homeland Security conducted a search of a former NASA contractor as part of an investigation of potential export control violations. Six weeks later, the individual pleaded guilty in Federal court to a misdemeanor offense of violating Agency security rules. On August 22, 2013, NASA's Office of Inspector General (OIG) issued a report of investigation titled "Bo Jiang's Access to NASA's Langley Research Center." This report was released to the public (with redactions) on October 22, 2013.⁴
- In a separate case, Federal law enforcement agencies received complaints dating back to 2009 that foreign nationals working as contractors at NASA's Ames Research Center were given improper access to facilities and sensitive information. These complaints led to a 4-year criminal investigation by the Federal Bureau of Investigation, the Department of Homeland Security, and the NASA Office of Inspector General, culminating in the forwarding of the case for prosecution to the U.S. Attorney for the Northern District of California. The criminal matter was not pursued; however the NASA IG continued the investigation as an administrative matter. On February 12, 2014, NASA's OIG issued a report titled "Review of International Traffic in Arms Regulations and Foreign National Access Issues at Ames Research Center." A brief summary of this report was released to the public on February 26, 2014.⁵

The issues highlighted in these reports were also corroborated by two separate, independent reviews:

- In January 2014, the National Academy of Public Administration issued a report titled "An Independent Review of Foreign National Access Management," which was requested by Rep. Frank Wolf. NASA has publicly released the executive summary of this report.⁶
- Last month, the Government Accountability Office released a report titled "Export Controls: NASA Management Action and improved Oversight Needed to Reduce the Risk of Unauthorized Access to its Technologies."⁷ This report was requested by Oversight Subcommittee Chairman Paul Broun on October 25, 2012.⁸

⁴ Accessed at http://oig.nasa.gov/Special-Review/OIG_Investigative_Summary.pdf

⁵ Accessed at http://oig.nasa.gov/Special-Review/Ames_ITAR.pdf

⁶ Accessed at http://www.nasa.gov/sites/default/files/files/NAPA_Executive_Summary_FNAM_Review_2014_Outlined-TAGGED-Final.pdf

⁷ Accessed at <http://www.gao.gov/products/GAO-14-315>

⁸ Accessed at <http://science.house.gov/letter/broun-letter-gao-comptroller-general-dodaro-nasa-export-controls>

Findings

The NASA OIG issued the following noteworthy findings in their two reports:⁹

- “We found that Langley’s process for requesting access for foreign nationals was structured pursuant to NASA regulations. However, we also found the process overly complex, required input from numerous Centers and headquarters employees, and not sufficiently integrated to ensure that responsible personnel had access to all relevant information.”
- “...we determined that several employees who have roles in the screening process made errors that contributed to the confusion about the proper scope of Jiang’s access to Langley facilities and IT resources and the appropriateness of Jiang taking his NASA-provided laptop to China.”
- “...we were struck by the highly bureaucratic nature of Langley’s process for reviewing foreign visit requests. Each of the many actors in the process appeared to view their role in isolation, with little consideration or understanding of the role others played in the process. In many instances, individuals seemed more focused on moving requests into the next person’s in-box than ensuring that their actions made sense in the context of the request they have been asked to review.”
- “In some instances, employees seemed to realize that they did not fully understand what they were doing or why they were doing it but proceeded anyway, assuming that someone else down the road would figure it out.”
- “...NIA appeared to lack sufficient procedures to ensure that appropriate officials in its organization were informed of the restrictions NASA placed on Jiang’s access to the Center [LaRC].”
- “From an individual perspective, the preponderance of evidence available to us suggests that one of Jiang’s sponsors inappropriately authorized Jiang to take the laptop to China.”
- “...we believe Jiang’s sponsor erred in not consulting Center export personnel before providing Jiang access to Rahman’s [NASA employee] hard drive or informing export officials they had done so in a timely manner.”
- “With respect to ITAR issues, we found that several foreign nationals without the required licenses worked on projects that were later determined to involve ITAR-restricted information.”
- “...on two occasions a senior Ames manager inappropriately shared documents with unlicensed foreign nationals that contained ITAR markings or had been identified as containing ITAR-restricted information by NASA export control personnel.”
- “We also found that a foreign national working at Ames inappropriately traveled overseas with a NASA-issued laptop containing ITAR-restricted information.”
- “...a senior official at Ames knew about and failed to stop a foreign national from recording conversations with Ames coworkers without their knowledge or consent, a practice that violated NASA regulations and California law.”
- “...we found that security rules designed to protect NASA property and data were not consistently followed in a rush to bring two foreign nationals on board at Ames. For example, contrary to NASA rules a foreign national improperly received unescorted

⁹ See *Supra* 4 and 5

access privileges to Ames in 2006 prior to the completion of required background checks and worked at the Center for nearly 3 years without a required security plan.”

- “In sum, we did not find intentional misconduct by any Ames civil servants but believe some Ames managers exercised poor judgment in their dealings with foreign nationals who worked on Center.”

The GAO made the following findings of note in their report last month:¹⁰

- “Weaknesses in implementation of NASA export control, foreign national access, and scientific and technical information procedures at some Centers creates export control vulnerabilities.”
- “Management decisions on Center Export Administrator authority, organizational placement, and resources affect export control implementation at Centers.”
- “We identified instances where NASA security procedures for foreign national access were not followed, which **were significant given the potential impact on national security** or foreign policy from unauthorized access to NASA technologies” [emphasis added].
- “...at one center, export control officials’ statements and our review of documentation showed that, in seven instances between March and July of 2013, foreign nationals fulfilled the role of sponsors – typically NASA project managers or other NASA officials who establish and endorse the need for a relationship between the foreign national and NASA and request their access to NASA facilities and information technology systems – by identifying the access rights to NASA technology for themselves and other foreign nationals for one NASA program.”
- “CEAs [Center Export Administrators] and Security officials from three centers cited instances where sponsors, escorts and personnel working at the facility being visited by foreign nationals are not aware of their roles and responsibilities of the provisos that detailed the level of physical and virtual access for the foreign national visitor.”
- “Based on our review of NASA’s most recent STI [Scientific and Technical Information] compliance audits, most centers continue to release STI that has not been reviewed for export control purposes.”
- “We did not assess STI documents that were not reviewed or information that was posted on NASA websites without export control review to determine if their release violated export controls, but without the completion of these reviews, **NASA is at increased risk of inadvertently releasing controlled technologies.**” [emphasis added]
- “NASA lacks a comprehensive inventory of export-controlled technologies and NASA Headquarters is not fully utilizing oversight tools”
- “...it is important to have clear export control policies that have strong management support and effective oversight to ensure consistent adherence across NASA Centers. **NASA’s program is lacking in both areas.**” [emphasis added]
- “When dealing with export controlled information, every instance of unapproved foreign national access or unapproved release of scientific information increases the risk of harm to national security.”

¹⁰ See *Supra* 7

The NAPA review issued the following notable findings:¹¹

- “The Academy found that there is little accountability for non-compliance when identified through specific incidents or periodic assessments. This validates the identified perception among NASA personnel that ‘mandatory compliance’ means little, as there are few, if any, consequences for deliberate or inadvertent violations of the mandates.”
- “Due to the fact that the NASA systems lack the necessary controls to protect information, allow foreign nationals access to the networks, and allow remote access, **the Panel concludes that the NASA networks are compromised.** Publicly available reports on systemic data breaches across the country, NASA’s own internal reports, and briefings given to Academy staff leave little doubt that information contained on the NASA IT systems is compromised.” [emphasis added]
- “NASA Headquarters (HQ) Officials and Center Directors have not adequately communicated that strict compliance was and is required for foreign national hosting, sponsoring, and escort policy and procedures.”
- “Directives, and orders, can be seen more as ‘guidance’ as opposed to mandatory policy and procedural requirements that must be adhered to. This can lead to communications breakdowns and negative outcomes.”
- “After fixing a problem, the Agency has a tendency to lapse back into old habits once the spotlight is off the area under review;”
- “A number of NASA leaders also noted that **the Agency tends not to hold individuals accountable even when they make serious, preventable errors.** Whenever an example of such an error was mentioned during the interviews, Academy staff would follow-up with: *what happened to those responsible for the error?* In almost every instance, the answer was either ‘nothing’ or ‘I don’t know’” [emphasis added]
- “Others [NASA centers] take a more *laissez-faire* approach with training either being optional or, if mandatory, provides no sanctions against those who fail to take the training”
- “In summary, the Panel found export control training requirements are inconsistent; the training is confusing and inadequate; and the rationale for such training is often poorly understood.
- “The Export Control program needs a more standardized and systematic approach in furtherance of its export compliance objectives, as well as better audit and review mechanisms. NASA senior leaders also need to more strongly endorse the critical importance of such controls.”
- “Specific intelligence regarding threats posed by foreign nationals and insiders to specific NASA assets is available from IC agencies, but has been inconsistently utilized to educate NASA personnel.”
- “NASA facilities, personnel, technologies, and information are highly regarded and of great interest to the world. That interest extends to some countries, governments, organizations, and individuals whose intent is to compromise those facilities, co-opt the personnel, and steal those technologies and information.”

¹¹ See *Supra* 6

Recommendations

The NASA OIG made six recommendations to improve NASA's foreign visitor approval process¹²:

1. "Examine the roles of the different offices that have input into the foreign visitor approval process and ensure that all appropriate offices are represented and that responsibilities are appropriately assigned.
2. Improve training for sponsors of foreign nationals to ensure they understand how the foreign national visit approval process works and their responsibilities as sponsors. This training should be required prior to an individual becoming a sponsor and be repeated at least annually as long as they continue to serve in this capacity.
3. Revise the Security Technology Transfer Control Plan (STTCP) to include NASA policy regarding taking information technology (IT) equipment out of the United States and ensure that employees are trained regarding this policy.
4. Consider the following improvements to IdMax [electronic database used to process foreign national access]:
 - a. Require individuals who will be acting as sponsors to acknowledge receipt of the plan and their understanding of all conditions placed on the visits of foreign nationals they are sponsoring; and
 - b. Prevent the system from generating final approval until all key documents, including the STTCP, are loaded into the system.
5. Ensure that the National Institute of Aerospace (NIA) and other similar organizations have a process in place so that appropriate organizational officials are aware of the many conditions NASA places on foreign nationals associated with their organizations who are working with NASA.
6. Consider whether discipline and/or performance-based counseling are appropriate for any of the NASA civil servants discussed in this report [related to Bo Jiang's access]."

The GAO issued the following recommendations:¹³

To ensure consistent implementation of NASA's export control program, GAO recommended that NASA:

1. "Establish guidance of defining the appropriate level and organizational placement of the CEA function.
2. Assess CEA workload and other factors to determine appropriate resources needed to support the CEA function at each Center."

GAO made five additional recommendations to improve NASA's oversight and address identified deficiencies in the export control program:

¹² See *Supra* 4

¹³ See *Supra* 7

1. "Implement a risk-based approach to the export control program by using existing information sources, such as counterintelligence assessments, to identify targeted technologies that are identified and managed by CEAs within each Center.
2. Direct Center Directors to oversee implementation of export-related audit findings which could involve collaboration among several Center offices.
3. Develop a plan, including timeframes for addressing CEA issues and suggestions for improvement provided during the annual export control conference, and share the plan with CEAs.
4. Re-emphasize to CEAs the requirements on how and when to notify the Headquarters Export Administrator about potential voluntary disclosures to ensure more consistent reporting of potential export control violations at NASA Centers.
5. Develop plans with specific time frames to monitor correction actions related to management of foreign national access to NASA facilities and assess their effectiveness."

NAPA made a total of 27 recommendations in their full report, which are summarized by the following topics:¹⁴

1. **"Manage FNAME as a Program.** The Panel proposed a number of steps for NASA to take which would begin to coordinate efforts and secure better results including realignment of both field and Headquarters organizational elements, strengthening the oversight capabilities of headquarters, and, improving training by developing comprehensive, integrated curriculums and lesson plans.
2. **Reduce the flexibility given to Centers to interpret FNAME requirements.** The Panel recommended that NASA Headquarters write a comprehensive and detailed FNAME operating manual covering all functional aspects of the program. Currently, FNAME directives can be found in several different publications, each with their own Headquarters and field constituencies. Headquarters staff should work in consultation with knowledgeable field staff to create this manual.
3. **Determine critical assets and build mechanisms to protect them.** The Panel envisions the creation of an Asset Protection Oversight Board which would use the results of the Independent Review Teams assessments of individual program compliance metrics as well as overall performance and outcomes of FNAME and the adequacy of the comprehensive threat/risk assessment at each Center.
4. **Correct longstanding information technology security issues.** The Panel believes NASA needs to identify and protect sensitive, proprietary information in a manner that does not prevent system owners from meeting their mission needs. Among the specific recommendations in this area are for NASA to establish clear, specific, and mandatory requirements for all Centers to follow regarding remote access of their information technology systems and that the NASA Chief Information Officer be given more control over IT operations in field Centers.
5. **Work to change several aspects of NASA culture.** Included in this are the recommendations to reduce unnecessary competition between field centers, ensure that accountability for conforming to FNAME requirements is established, and finally, to guard against the organizational tendency to revert back to prior lax habits once a problem area has been addressed.

¹⁴ See *Supra* 6

6. **Communicate the importance of these FNAM changes clearly, firmly and consistently.** The importance of security, the existence of “real world” threats to NASA assets, and the need for improvements in handling foreign national issues have not been clearly and consistently communicated throughout NASA. Senior leaders must firmly establish and communicate their total commitment to an effective Foreign National Access Management program that enhances cooperation while safeguarding information.”

Chairman PALAZZO. This joint hearing of the Subcommittee on Space and the Subcommittee on Oversight will come to order.

Good morning. Welcome to today's hearing titled, "NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information." In front of you are packets containing the written testimony, biography, and truth-in-testimony disclosure for today's witnesses.

Before we get started, since this is a joint hearing involving two Subcommittees, I want to explain how we will operate procedurally so all Members understand how the question-and-answer period will be handled. We will recognize those Members present at the gavel in order of seniority on the full Committee, and those coming in after the gavel will be recognized in order of arrival.

I recognize myself for five minutes for an opening statement.

Welcome to today's joint hearing on NASA's ability to protect sensitive information. Recent events have reminded us that protecting sensitive aerospace information is more than a matter of national pride; it is also a matter of national security. Yet NASA continues to struggle with the protection of sensitive information, even as the agency is persistently targeted by our adversaries.

Today, we discuss the reports that have shown that NASA's casual and negligent approach to foreign national access and failure to control sensitive information is allowing our nation's prized aerospace technology to be compromised. The purpose of today's hearing is to ensure that NASA follows through on addressing these failures.

On March 16, 2013, Federal agents conducted a search of a foreign national contractor from the Langley Research Center before departure to China. This search was prompted by concerns that the individual was inappropriately granted access to sensitive information. Despite the fact that the individual pled guilty to a misdemeanor offense, the nature of the information on his computer and how he obtained it remains under investigation.

Also, a multiyear investigation dating back to 2009 showed that foreign nationals were granted inappropriate access to information and facilities at NASA's Ames Research Center. As a result, NASA's Office of the Inspector General issued a detailed 41-page report highlighting troubling cases where improper access was granted under direction from senior center leadership.

Today's hearing is one in a series of Congressional actions to address these matters. In addition to a hearing held last Congress in this Committee, Dr. Paul Broun, Chairman of the Oversight Committee, requested a GAO review of NASA's export control processes. And Representative Frank Wolf petitioned NASA to work with the National Academy of Public Administration to conduct an independent review of NASA's Foreign National Access Management. Unfortunately NASA has only released a summary of this report.

These reports confirm our worst fears: that the incidents at Langley and Ames are not isolated incidents. Among conclusions from these reports we find most centers continue to release scientific and technical information that has not been reviewed for export control purposes. NASA lacks both clear export control policies and the oversight necessary to enforce them. The NASA network

has indeed been compromised and these vulnerabilities could have significant impacts on national security.

And finally, a troubling trend we have seen across agencies in this Administration: the failure or the willingness—unwillingness to hold accountable those responsible for these errors.

Congress has also continued addressing these matters in the NASA Authorization Act that recently passed the House by an overwhelming bipartisan vote of 401 to 2. Our bill directs NASA to give a timely report on compliance efforts in response to the recommendations of the NAPA report. It also calls for a GAO review of NASA's compliance and directs NASA to take national security into consideration when conducting technology transfers.

My goal as Chairman of this Committee is to hold NASA accountable while working with the agency to correct these serious matters. I understand that NASA has its challenges. The original Space Act directed the agency to simultaneously “provide for the widest practicable and appropriate dissemination of information concerning its activities” while also directing the agency to protect classified, trade secret, and confidential information.

Additionally, NASA, like other Federal agencies, is subject to the requirements of the Arms Export Control Act and the Export Administration Act. Too often, enforcement is left to the discretion of center leadership in a NASA culture that “has a tendency to lapse back into old habits once the spotlight is off the area under review.” I will point out that this is more than my personal assessment; it is the independent opinion as expressed in the NAPA report.

I am pleased that NASA's Office of the Inspector General is here today to discuss these two reports, as well as their yearly report to Congress on NASA's compliance with Federal export controls laws. I am also pleased that two other outside groups have also reviewed the topic, the National Academy of Public Administration and GAO.

While much of the focus of today's hearing will be to identify the failures within NASA's current structure, it is also an opportunity to identify ways Congress can improve and clarify its own roles in providing oversight and accountability over NASA activities. I believe this is in the best interest of all involved as we look to the future in a world where our nation's space interests are impacted by both the cooperation and competition of international players.

[The prepared statement of Mr. Palazzo follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON SPACE
CHAIRMAN STEVEN M. PALAZZO

Welcome to today's joint hearing on NASA's ability to protect sensitive information.

Recent events have reminded us that protecting sensitive aerospace information is more than a matter of national pride; it is also a matter of national security. Yet, NASA continues to struggle with the protection of sensitive information, even as the agency is persistently targeted by our adversaries. Today we discuss the reports that have shown that NASA's casual and negligent approach to foreign national access—and failure to control sensitive information—is allowing our Nation's prized aerospace technology to be compromised. The purpose of today's hearing is to ensure that NASA follows through on addressing these failures.

On March 16, 2013 federal agents conducted a search of a foreign national contractor from the Langley Research Center before departure to China. This search

was prompted by concerns that the individual was inappropriately granted access to sensitive information. Despite the fact that the individual pled guilty to a misdemeanor offense, the nature of the information on his computer, and how he obtained it, remains under investigation.

Similarly, a multi-year investigation dating back to 2009 showed that foreign nationals were granted inappropriate access to information and facilities at NASA's Ames Research Center. As a result, NASA's Office of the Inspector General issued a detailed 41 page report highlighting troubling cases where improper access was granted under direction from senior center leadership. Today's hearing is one in a series of congressional actions to address these matters. In addition to a hearing held last Congress in this Committee, Dr. Paul Broun, Chairman of the Oversight Committee requested a GAO review of NASA's export control processes. And Rep. Frank Wolf petitioned NASA to work with the National Academy of Public Administration (NAPA) to conduct an independent review of NASA's foreign national access management. Unfortunately NASA has only released a summary of this report.

These reports confirm our worst fears: that the incidents at Langley and Ames are not isolated incidences. Among conclusions from these reports we find: most centers continue to release Scientific and Technical Information that has not been reviewed for export control purposes. NASA lacks both clear export control policies and the oversight necessary to enforce them. The NASA network has indeed been compromised, and these vulnerabilities could have significant impacts on national security. And finally, a troubling trend we've seen across agencies in this Administration: the failure or the unwillingness to hold accountable those responsible for these errors.

Congress has also continued addressing these matters in the NASA Authorization Act that recently passed the House by an overwhelming bipartisan vote of 401 to 2. Our bill directs NASA to give a timely report on compliance efforts in response to the recommendations of the NAPA report. It also calls for a GAO review of NASA's compliance and directs NASA to take national security into consideration when conducting technology transfers.

My goal as Chairman of this Committee is to hold NASA accountable while working with the agency to correct these serious matters. I understand that NASA has its challenges: the original Space Act directed the agency to simultaneously "provide for the widest practicable and appropriate dissemination of information concerning its activities" while also directing the agency to protect classified, trade secret, and confidential information. Additionally, NASA—like other federal agencies—is subject to the requirements of the Arms Export Control Act and the Export Administration Act. Too often, enforcement is left to the discretion of center leadership in a NASA culture that "has a tendency to lapse back into old habits once the spotlight is off the area under review." I will point out that that is more than my personal assessment— it is the independent opinion as expressed in the NAPA report.

I am pleased that NASA's Office of the Inspector General is here today to discuss these two reports, as well as their yearly report to Congress on NASA's compliance with federal export controls laws. I am also pleased that two other outside groups have also reviewed the topic—National Academy of Public Administration (NAPA) and GAO. While much of the focus of today's hearing will be to identify the failures within NASA's current structure, it is also an opportunity to identify ways Congress can improve and clarify its own roles in providing oversight and accountability over NASA activities. I believe this is in the best interest of all involved as we look to the future in a world where our nation's space interests are impacted by both the cooperation and competition of international players.

Thank you.

Chairman PALAZZO. I now recognize Mr. Maffei, who—are you going to be doing Ms. Edwards' statement or are you just going to go straight into your statement?

Mr. MAFFEI. I am just going to go straight into mine, I think.

Chairman PALAZZO. Yes. Okay. Good.

Mr. MAFFEI. Thank you, Mr. Chairman. Thank you Chairman Palazzo. Ms. Edwards does apologize. She was unavoidably detained and will be a little late. I for one though am pleased to see two Italian-American names up here, so, you know, a lot of our space technology has a lot to owe to Italy and history there.

I won't talk long and actually I ask unanimous consent to put my full statement in the record. I want to put my full statement in the record by unanimous consent and then I will just talk for a minute.

Chairman PALAZZO. Without objection.

[The prepared statement of Mr. Maffei follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON OVERSIGHT
RANKING MINORITY MEMBER DAN MAFFEI

Thank you Chairman Palazzo and Chairman Broun for holding this hearing today.

Ensuring that America's sensitive technical designs and security related research is not intentionally pilfered or inappropriately exported is important to this nation's economic and national security. Each year the U.S. loses billions of dollars' worth of advanced technologies, innovative scientific research, and other sensitive data due to economic espionage and data theft.

This impacts U.S. businesses as well as U.S. government laboratories and research centers. NASA is no exception. The National Aeronautics and Space Administration (NASA), like other federal agencies, is a prime target of foreign agents and global cyber criminals.

The agency has a lot to offer. NASA leads the world in space exploration, aeronautics research, and other key scientific areas. Controlling the inadvertent release of sensitive information or intentional theft of export controlled technologies has always been a difficult task. This is particularly true when that sort of data resides in an environment that depends upon international collaborations and access to foreign scientists and facilities. Over its history NASA has had more than 3,000 international cooperative agreements and currently maintains an estimated 600 international agreements with more than 100 foreign countries. Last year NASA approved more than 11,000 foreign national visits to its facilities. At a time of constrained federal budgets and reductions in investments in science and technology, NASA is dependent upon these global interactions to ensure its continued success.

Unfortunately, NASA has suffered from several security incidents in recent years that sparked reviews of its security policies and practices. These reviews by the Government Accountability Office (GAO), NASA's Office of Inspector General and the National Academy of Public Administration (NAPA) have all identified poor practices in protecting sensitive NASA technologies, organizational issues that may undermine NASA's security protocols, and financial constraints that may contribute to the inadvertent release of export restricted data. NASA was fortunate, however, that the incidents themselves do not appear to have resulted in major losses of sensitive data.

In one of the most high profile cases involving Chinese national Bo Jiang, who was accused of attempting to take a NASA laptop to China without proper authorization while working at NASA's Langley Research Center in Virginia, federal prosecutors found that, "none of the computer media that Jiang attempted to bring to [China] on March 16, 2013, contained classified 2 information, export-controlled information, or NASA proprietary information." In a separate incident involving two foreign nationals working at NASA's Ames Research Center in California a NASA Inspector General report released in February, "uncovered no evidence to support allegations that any foreign nationals at Ames were provided classified information during the period covered by our review."

NASA was lucky it did not sustain a serious loss of critical data or technology, but the space agency has unique national assets, innovative technologies, and valuable scientific data that must be properly protected from global economic competitors, foreign adversaries, or individual theft by those seeking to cash in on the agency's valuable research and innovative discoveries.

Being able to detect and deter these security threats while at the same time supporting important international scientific collaborations is a delicate and often difficult balance to achieve. I look forward to our witnesses helping us to better understand these issues, evaluating these often conflicting objectives, and recommending ways to maintain an appropriate balance.

Mr. MAFFEI. Ensuring that America's sensitive technical designs and security-related research is not intentionally pilfered or inappropriately exported is extremely important to this nation's economic and national security, and that is why I am so grateful to

Chairman Palazzo and Chairman Broun for holding this hearing today. It is an extremely important issue.

Each year, the United States loses billions of dollars worth of advanced technologies, innovative scientific research, and other sensitive data due to economic espionage and data theft, and this impacts U.S. businesses as well as government laboratories and research centers. And NASA, like other Federal agencies, is a prime target for this type of espionage. Being able to detect and deter these security threats while at the same time supporting important international scientific collaboration is a delicate and often difficult balance to achieve.

And I particularly look forward to hearing from our witnesses to help us better understand these issues, how we set that balance, and evaluate sometimes conflicting objectives to recommend the right way to do it.

So thank you very much, and with that I will yield back.

Chairman PALAZZO. Thank you, Mr. Maffei.

I now recognize Dr. Broun, Chairman of the Oversight Committee.

Mr. BROUN. Thank you, Chairman Palazzo.

I would like to add my welcome to all of you all witnesses that are here today as well. I am looking forward to hearing from you about this important matter of which I have been concerned for a number of years now.

This Committee and the Oversight Subcommittee in particular have held multiple hearings examining the state of information security at NASA. A hearing two years ago highlighted the unique cybersecurity challenges that NASA continues to face with constant and ever-changing threats and adversaries. Just last year, the Oversight Subcommittee, which I Chair, held a hearing to focus on the broad intersection of two very important issues at stake here today: finding the appropriate balance between scientific openness and protecting our national security.

We have learned that NASA should not only worry about sensitive information going out of the back door through cyber intrusions and lax protocols but also out of the front door by its inability to protect sensitive technology and information from foreign nationals who may have unauthorized access to NASA's facilities.

In October of 2012, I wrote to the GAO regarding these front-door concerns and requested a review of NASA's export control program. While I was glad to see the completed GAO report released last month, I was troubled by many of the report's findings. For example, it is very troubling to learn that although NASA's oversight tools have identified deficiencies, NASA headquarters has not addressed them at all as far as I can tell.

The GAO report states specifically that "at NASA's 2013 annual review, the Center Export Administrators presented NASA HC export control officials with a list of comments regarding the export control program. However, NASA headquarters' export control officials acknowledged that they have not fully addressed the CEA concerns from the most recent program review in March of 2013 and have not developed specific plans to do so." This is intolerable. This is not because of any disagreement between NASA headquarters' staff and NASA centers' staff; in fact, the GAO report ex-

plains that NASA headquarters export control officials agree with issues raised by the CEAs, yet they have failed to develop an approach to address them. This is wholly inadequate for protecting our valuable assets. NASA needs suitable accountability and oversight in order to, at the very least, make certain the agency's own audit findings and suggestions are implemented.

Further troubling, the report states the GAO "identified instances where NASA security procedures for foreign national access were not followed, which were significant given the potential impact on national security or foreign policy from unauthorized access to NASA technologies."

NASA relies on new and sophisticated technology to accomplish its mission. Given the sensitivity of these technologies, many are subject to export controls, which restrict the transfer of military and dual-use technologies. In order to protect our leadership in technological innovations, we must ensure that there is adequate and consistent oversight and management of NASA's export control program. It is in our national interest. It must be done.

I look forward to hearing from our witnesses on their insight and recommendations on these matters, and I hope that NASA will do everything in its power to address all of the shortcomings discussed today to ensure our nation's space agency can securely support and appropriately protect cutting-edge research and technology.

Thank you, Chairman Palazzo, for holding this very important hearing, and I yield back the balance of my time.

[The prepared statement of Mr. Broun follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON OVERSIGHT CHAIRMAN PAUL BROUN

Assessing the Agency's Efforts to Protect Sensitive Information Chairman Broun: Thank you Chairman Palazzo. I would like to add my welcome to all of our witnesses here today as well. I am looking forward to hearing from you all on this important matter of which I have been concerned for a number of years now.

This Committee and the Oversight Subcommittee, in particular, have held multiple hearings examining the state of information security at NASA. A hearing two years ago highlighted the unique cybersecurity challenges that NASA continues to face with constant and ever-changing threats and adversaries. Just last year, the Oversight Subcommittee held a hearing to focus on the broad intersection of two very important issues at stake here today - finding the appropriate balance between scientific openness, and protecting our national security.

We have learned that NASA should not only worry about sensitive information going out of the back door through cyber intrusions and lax protocols, but also out of the front door by its inability to protect sensitive technology and information from foreign nationals who may have unauthorized access to NASA's facilities.

In October of 2012, I wrote to the GAO regarding these front door concerns and requested a review of NASA's export control program. While I was glad to see the completed GAO report released last month, I was troubled by many of the report's findings. For example, it is very troubling to learn that although NASA's oversight tools have identified deficiencies, NASA headquarters has not addressed them. The GAO report states specifically that "at NASA's 2013 annual review, the Center Export Administrators presented NASA headquarters export control officials with a list of comments regarding the export control program. However, NASA headquarters' export control officials acknowledged that they have not fully addressed the CEA concerns from the most recent program review in March 2013 and have not developed specific plans to do so." This is intolerable. This is not because of any disagreement between NASA headquarters' staff and NASA centers' staff; in fact the GAO report explains that NASA headquarters export control officials agree with issues raised by the CEAs—yet, they have failed to develop an approach to address them.

This is wholly inadequate for protecting our valuable assets. NASA needs suitable accountability and oversight in order to, at the very least, make certain the agency's own audit findings and suggestions are implemented.

Further troubling, the report states that GAO "identified instances where NASA security procedures for foreign national access were not followed, which were significant given the potential impact on national security or foreign policy from unauthorized access to NASA technologies."

NASA relies on new and sophisticated technology to accomplish its mission. Given the sensitivity of these technologies, many are subject to U.S. export controls, which restrict the transfer of military and dual-use technologies. In order to protect our leadership in technological innovations, we must ensure that there is adequate and consistent oversight and management of NASA's export control program. It is in our national interest. It must be done!

I look forward to hearing from our witnesses on their insight and recommendations on these matters, and I hope that NASA will do everything in its power to address all of the shortcomings discussed today to ensure our nation's space agency can securely support and appropriately protect cutting edge research and technology.

Thank you again Chairman Palazzo for holding this very important hearing, and I yield back the balance of my time.

Chairman PALAZZO. Thank you, Dr. Broun.

I now recognize the Ranking Member of the full Committee for a statement, Ms. Johnson.

Ms. JOHNSON OF TEXAS. Thank you very much, Mr. Chairman. And let me say good morning to all.

In the interest of saving time, I will be brief so that our distinguished panel of witnesses will have time to present their views.

I will say that civil R&D requires openness, collaboration, and sharing of results to be successful. NASA's R&D portfolio has benefited from the culture of openness, but the benefits of that culture of openness, collaboration, and sharing must be balanced with appropriate security limit and protections. This can be a constructive hearing, especially if we can find ways to enable NASA to strike a reasonable balance between information sharing and the need to safeguard any sensitive information and technologies from inadvertent disclosure.

I look forward to discussing this and other issues with our expert panel since the issues being addressed today are many of the same challenges that confront the other science agencies under the Committee's oversight umbrella. And so with that, Mr. Chairman, I yield back.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF FULL COMMITTEE
RANKING MEMBER EDDIE BERNICE JOHNSON

Good morning. In the interest of saving time, I will be brief so that our distinguished panel of witnesses will have time to present their views.

Civil R&D requires openness, collaboration, and sharing of results to be successful. NASA's R&D portfolio has benefitted from that culture of openness. But the benefits of that culture of openness, collaboration, and sharing must be balanced with appropriate security limits and protections.

This can be a constructive hearing, especially if we can find ways to enable NASA to strike a reasonable balance between information sharing and the need to safeguard any sensitive information and technologies from inadvertent disclosure.

I look forward to discussing this and other issues with our expert panel, since the issues being addressed today are many of the same challenges that confront the other science agencies under the Committee's oversight umbrella.

With that, I yield back.

Chairman PALAZZO. Thank you, Ms. Johnson.

If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

Chairman PALAZZO. At this time I would like to introduce our witnesses.

Our first witness, Mr. Richard Keegan, is the National Aeronautics and Space Administration's Associate Deputy Administrator and Associate Administrator for Mission Support. Our second witness, Ms. Belva Martin, is the Director of Acquisition and Sourcing Management at the Government Accountability Office. Our third witness, Ms. Gail Robinson, is the Deputy Inspector General of the National Aeronautics and Space Administration. And our final witness, Mr. Douglas Webster, is a Fellow of the National Academy of Public Administration and the Principal at Cambio Consulting Group.

As our witnesses should know, spoken testimony is limited to five minutes each after which the Members of the Committee will have five minutes each to ask questions. It is the practice of the Subcommittee on Oversight to receive testimony under oath. If you would now please stand and raise your right hand.

Do you solemnly swear or affirm to tell the whole truth and nothing but the truth, so help you God?

Please sit.

Let the record reflect that all witnesses participating have taken the oath.

I now recognize Mr. Keegan for five minutes.

**TESTIMONY OF MR. RICHARD KEEGAN,
ASSOCIATE DEPUTY ADMINISTRATOR,
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION**

Mr. KEEGAN. Mr. Chairman and Members of today's respective Subcommittees, I am pleased to have this opportunity to discuss NASA's efforts to manage and safeguard the agency's export-controlled technologies and information from unauthorized access and use. This is a topic which we agree is of great importance to our Nation.

As the world's premier aerospace agency with expertise in space launch vehicles, satellites, aircraft, and other advanced technologies, NASA takes our responsibility for securing sensitive export-controlled information at our facilities very seriously. To be clear, all NASA employees have a responsibility to comply with export control regulations and Foreign National Access Management requirements. That is why the NASA Administrator himself has communicated to every employee that these requirements are critically important and that there will be appropriate consequences for those who fail to appropriately safeguard sensitive technologies and information.

The recent independent reviews that will form the basis of today's hearing have already provided invaluable guidance to the agency in our efforts to protect sensitive information and to improve our Information Technology Security, Foreign National Access Management, and Export Control Management programs. Therefore, NASA is working to implement these recommendations

in an expeditious manner, beginning immediately. In parallel, NASA will continue to improve and implement appropriate policy and process changes that we ourselves identify during our own internal audits and reviews.

Cooperation with other nations is one of the agency's founding principles and thus we would like to thank the GAO and NAPA for recognizing this core principle during their recent reviews about NASA security issues. In doing so, these independent reviewers also highlighted the need for NASA to strike the right balance between protecting sensitive export-controlled technologies from unauthorized access and the need for the agency to share important scientific information to further our public and international partnerships. In striking the appropriate balance, NASA recognizes that the agency must have clear export control policies and procedures and that all NASA employees must understand and abide by those policies and procedures.

NASA is redoubling our efforts to ensure that we are doing all we can to safeguard the sensitive and valuable resources entrusted to us. As specific examples, NASA is working to improve training for employees who deal with export control and foreign nationals. We have established a new Foreign National Access Management program office. We are strengthening our foreign national access and export control policies and procedures. We are augmenting the civil service staff dedicated to counterintelligence activities. And we are increasing collaboration with other Federal agencies to share intelligence on threats and vulnerabilities to our information technology and other assets.

In conclusion, let me assure you that NASA takes seriously our responsibility to secure sensitive export-controlled information. Additionally, the agency's security issues and threats will continue to have the focused attention of NASA's most senior managers, including the Administrator himself.

Lastly, NASA will continue to follow through on the valuable recommendations made by the GAO, NAPA, and our own Inspector General with regard to these issues.

Thank you for the opportunity to testify before you today and for your ongoing support for NASA's missions and its workforce. I would be pleased to answer any questions you may have.

[The prepared statement of Mr. Keegan follows:]

HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
June 20, 2014

Statement of
Mr. Richard Keegan
Associate Deputy Administrator
National Aeronautics and Space Administration

before the
Subcommittee on Space
and
Subcommittee on Oversight
Committee on Science, Space and Technology
U. S. House of Representatives

Mr. Chairmen and Members of today's respective Subcommittees, I am pleased to have this opportunity to discuss NASA's efforts to manage and safeguard the Agency's export-controlled technologies and information from unauthorized access and use. The recent independent reviews that form the basis of this hearing provide invaluable guidance in support of the Agency's efforts to protect sensitive information.

As the world's premier aerospace Agency with expertise in space launch vehicles, satellites, aircraft and other advanced technologies, we recognize that NASA has a unique responsibility to safeguard sensitive technologies. As NASA employees, we have each been entrusted with access to valuable resources, talent, capabilities and technologies, all of which demand careful stewardship, including compliance with the Nation's export control laws, regulations, and policies.

Cooperation with other nations is one of NASA's founding principles. The Agency has always sought the widest practical and appropriate distribution of information about our programs. Accordingly, the NASA Export Control Program is devoted to maximizing the benefits of our international and informational efforts while ensuring that we comply with all U.S. export control laws and regulations. The continuing success of this program for the protection of sensitive technologies is the personal responsibility of all NASA employees and a responsibility that every NASA manager, right up to and including the Administrator himself, takes very seriously.

Indeed, just last month, Administrator Bolden directly addressed those officials from across the Agency who manage the implementation of NASA's Export Control Program about the critical role they play in safeguarding sensitive NASA technologies. He also issued a communication to all NASA employees reminding them of their responsibility to comply with all export control regulations and foreign national access management requirements. His message stressed that safeguarding sensitive information is a serious matter and that penalties for noncompliance can include fines and imprisonment, as well as administrative personnel actions, such as reduction-in-grade or even termination. The Administrator also encouraged employees to meet with their local export control officials to learn more about NASA's Export Control Program and their responsibilities in protecting sensitive technologies. From the Agency's top management down to its newest employee, we are redoubling our efforts to perfect export control compliance through enhanced communication and training.

NASA Export Control Program

Established in 1995, the NASA Export Control Program, one of the first of its kind in the Federal Government, is an Agency-wide system established to ensure that exports and transfers to foreign parties in the course of approved international activities are consistent with the U.S. Export Administration Regulations (EAR) administered by the U.S. Department of Commerce and the International Traffic in Arms Regulations (ITAR) administered by the U.S. Department of State. Using proven policies and procedures, the NASA Export Control Program provides essential safeguards at key steps throughout NASA's program development and implementation process in a manner that supports robust international cooperation and foreign national access to NASA. Specifically, the NASA Export Control Program provides requirements, instructions and responsibilities for all NASA employees and support contractors engaged in activities that involve the transfer of commodities, software, or technologies to foreign individuals or organizations on behalf of the Agency. To implement this program NASA relies on a network of designated and fully trained export control administrators and counsel located at every NASA Field Center and NASA Headquarters. The longstanding success of this program can also be attributed to a well-established system of annual independent audits and voluntary self-disclosure of errors or noncompliance with export activities.

Recent Reviews

In April 2014, the Government Accountability Office (GAO) released its report entitled "Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the Risk of Unauthorized Access to its Technologies." The GAO report complements a review conducted by the National Academy of Public Administration (NAPA), which provided its final report to NASA in February 2014.

Following its review of NASA's Export Control Program and the management functions of that program, the GAO made seven recommendations intended to ensure consistent implementation and improve oversight, including the establishment of guidance to define the appropriate rank and organizational placement of those who manage the NASA Export Control Program at our Centers, taking better advantage of resources to identify targeted technologies, having NASA's Center Directors oversee implementation of our annual internal export control audit recommendations, addressing issues and suggestions for improvement provided during our annual Export Control Program Review, clarifying requirements on how and when to report potential voluntary disclosures, assessing export control management workload and resources, and developing plans to monitor improvements in NASA's Foreign National Access Management (FNAM) program. NASA concurred with each of these recommendations and immediately began work to implement them in a timely manner. The Agency anticipates completion of most actions by next spring, and will provide a 60-day progress report to the GAO and the relevant Congressional Committees by July 15, 2014. The NASA initial response to the GAO report is enclosed as Enclosure 1.

In March 2013, NASA commissioned a focused independent security review by the NAPA to assess the effectiveness of selected aspects of NASA programs and processes relevant to foreign national access management. NASA received the final NAPA report, entitled "An Independent Review of Foreign Access Management" in February 2014. The NAPA review focused on five areas: Information Technology, Security, Counterintelligence, Export Control and Organizational and Functional Relationships. NASA is fully engaged in responding to the recommendations in the NAPA report using a risk-based prioritization. NASA will systematically and incrementally address the NAPA recommendations and the identified risks through a series of initiatives executed in accordance with a

multi-year program, with the ultimate goal of substantially strengthening foreign national access management across the Agency. As part of the Agency's response to the NAPA report, NASA on March 10, 2014, established a FNAM Program within the Office of Protective Services. The FNAM Program will work to increase the efficiency and effectiveness of NASA processes and procedures and develop and implement improved procedures as required. The Program will also ensure that clear and consistent guidance is provided for FNAM activities across the Agency. On April 2, 2014, the Program established an interim policy strengthening Agency-wide guidance with respect to FNAM. NASA is working to incorporate this strengthened guidance in an update to its procedural requirements for identity and credential management. NASA's initial response to the NAPA report is enclosed as Enclosure 2.

NASA takes the responsibility of securing sensitive, export-controlled information at our facilities very seriously. Prior to receiving copies of the GAO report and the NAPA review, Administrator Bolden had already directed a number of actions to further secure sensitive, export-controlled information at NASA facilities in order to enhance overall security, consistent with recommendations made in recent reviews conducted by the NASA Office of the Inspector General (OIG). NASA's active responses to the GAO, OIG, and NAPA recommendations are assisting in our continuing efforts to enhance all aspects of NASA's foreign national access management, as well as NASA's export control compliance program.

The Proposed NASA FOIA Exemption

Last year, NASA submitted a legislative proposal to our authorization committees that is relevant to our shared export control focus. If adopted, the proposal would authorize NASA to withhold from public disclosure certain technical data with aeronautic or space application from release under the Freedom of Information Act (FOIA) if such data may not be exported lawfully outside the United States without an approval, authorization, or license under the provisions of the Export Administration Act (EAA) of 1979 or the Arms Export Control Act (AECA) of 1976. At present, there is no particular exemption in the FOIA that applies to export-controlled information under the EAA and AECA, nor is there any statute that specifically allows NASA to withhold it from public disclosure, which could include release to non-U.S. persons. The new statutory authority NASA has requested would put the Agency on par with the U.S. Department of Defense, which is able, through its own Title 10 provisions, to protect export-controlled information from public disclosure. NASA is requesting this new statutory authority in order to protect export-controlled information in its possession from public disclosure, and we would therefore appreciate the Subcommittee's support for this authority as the reauthorization continues through the legislative process.

Conclusion

In conclusion, I would like to thank you for this opportunity to testify today and note our agreement with the GAO's core finding – that it is important for the Agency to strike the right balance between needing to protect sensitive export-controlled technologies and information, and the Agency's need to share important scientific information to further our international and public partnerships. In striking the appropriate balance, NASA recognizes that we must have clear export control policies and that all NASA employees must understand and abide by those policies and procedures designed to protect sensitive technologies whose loss or theft could have grave national security implications. NASA will continue to follow through on the recommendations made by the GAO, NAPA, and our own Inspector General to safeguard access to NASA facilities by foreign nationals and to improve the protection of sensitive technologies. We will also continue to implement appropriate changes that we ourselves identify in the course of our own internal audits and reviews.

National Aeronautics and Space Administration
Headquarters
 Washington, DC 20546-0001



Reply to Attn of:

ENCLOSURE 1

Office of International and Interagency Relations

Ms. Belva Martin
 Director
 Acquisition and Sourcing Management
 United States Government Accountability Office
 Washington, DC 20548

Dear Ms. Martin:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the Risk of Unauthorized Access to Its Technologies" (GAO-14-315) dated March 7, 2014.

In the draft report, GAO makes seven recommendations to the NASA Administrator intended to ensure consistent implementation and improve oversight of NASA's export control program. NASA takes the responsibility of securing sensitive, export-controlled information at our facilities very seriously. Recognizing the growing threat of espionage aimed at Government agencies by hostile nation-states and foreign adversaries, the NASA Administrator has already directed a number of actions to further secure sensitive, export-controlled information at NASA facilities and to enhance overall security.

The draft GAO report complements recent reviews conducted by the NASA Office of the Inspector General in October 2013 and the National Academy of Public Administration (NAPA), which provided its findings to the NASA Administrator in January 2014. Each of these recent reviews evaluated the effectiveness of select aspects of NASA programs relevant to Foreign National Access Management. At the request of the NASA Administrator, the NAPA review focused on five areas: Information Technology, Security, Counterintelligence, Export Control, and Organizational and Functional Relationships. Your recommendations, together with those previously provided to NASA, are assisting in our continuing efforts to enhance all aspects of our Foreign National Access Management, including NASA's export control compliance program.

With regard to the specific recommendations contained in the GAO's draft report, NASA provides the following responses, including planned corrective actions:

Recommendation 1: Establish guidance defining the appropriate level and organizational placement of the CEA function.

Management's Response: NASA concurs. We will revise the NASA Procedural Requirements (NPR 2190.1B) governing the NASA Export Control Program (ECP) to specify the level of senior-level officials, at GS-15 or above, for the Center Export Administrator (CEA) function. We will also require that CEAs report directly to Center Directors or designees in the performance of their functions. Coupled with this, NASA will address a related recommendation from the January 2014 NAPA report that a Headquarters (HQ) endorsement be sought before any CEA position is filled by working with the human resources and Center management to ensure that NASA HQ endorsement is obtained for CEA appointments.

Estimated Completion Date: April 30, 2015.

Recommendation 2: Assess CEA workload and other factors to determine appropriate resources needed to support the CEA function at each Center.

Management's Response: NASA concurs. We have already begun to assess the need for additional resources to support the CEA function, with the understanding that, like all agencies, we are in a very constrained budget environment. We will explore strategies to enhance support of export control functions through both civil service and contractor efforts, and will work to expand the model of Center Export Control Representatives (ECRs) that has been successfully employed at more than half of NASA's Centers, and which was noted in the draft report.

Estimated Completion Date: April 30, 2016.

Recommendation 3: Implement a risk-based approach to the export control program by using existing information sources, such as counterintelligence assessments, to identify targeted technologies and then direct that the types and location of those export-controlled technologies are identified and managed by CEAs within each Center.

Management's Response: NASA concurs. Consistent with the recommendation, we will implement a risk-based approach for targeted technologies of particular concern, working with CEAs, program managers, and counterintelligence professionals to identify key technologies and catalog those key technologies at each Center. This balanced, focused approach follows the discussion on page 20 of the draft report and should not require significant additional resources to implement.

This recommendation is also consistent with the NAPA report's recommendation that NASA provide a detailed export control manual to serve as a standardized guide to CEAs, ECRs, and Center project managers, and to mandate the use of certain practices that have proven effective at various Centers. Subject to additional funding availability, NASA plans to develop an

export control manual in order to ensure greater consistency in implementation of the NASA ECP across the Agency. We will include provisions for a dynamic, risk-based assessment of key technologies in the manual.

Estimated Completion Date: First-draft of a manual to be prepared by April 30, 2015.

Recommendation 4: Direct Center Directors to oversee implementation of export-related audit findings which could involve collaboration among several Center offices.

Management's Response: NASA concurs. We will revise NPR 2190.1B to specify that Center Directors shall oversee the completion of annual ECP audits, and report their implementation or progress to the Associate Administrator for International and Interagency Relations (OIIR) and to the NASA Headquarters Export Control Administrator (HEA).

Estimated Completion Date: April 30, 2015.

Recommendation 5: Develop a plan, including timeframes for addressing CEA issues and suggestions for improvement provided during the annual export control conference, and share the plan with CEAs.

Management's Response: NASA concurs. This is a subject that will be addressed at the forthcoming Annual NASA ECP Review at Langley Research Center in May 2014. Following the engagement and agreement with CEAs on the subject, the HEA will formulate the recommended plan for inclusion in revisions to NPR 2190.1B.

Estimated Completion Date: April 30, 2015.

Recommendation 6: Re-emphasize to CEAs the requirements on how and when to notify the HEA about potential voluntary disclosures to ensure more consistent reporting of potential export control violations at NASA Centers.

Management's Response: NASA concurs. We will revise NPR 2190.1B to clarify the thresholds and standards for reporting voluntary disclosures to the HEA. Because of the linkage to both effective NASA ECP operations and to the NAPA report's recommendation to develop an export control manual in order to ensure greater consistency of proven best practices, we will also include provisions regarding voluntary disclosure standards in an export control handbook which we expect to produce. The timeline for the development of this handbook will be driven by the availability of additional resources.

Estimated Completion Date: April 30, 2015.

Recommendation 7: Develop plans with specific time frames to monitor corrective actions related to management of foreign national access to NASA facilities and assess their effectiveness.

Management's Response: NASA concurs. Under NASA Policy Directive (NPD) 2190.1, the Export Control Manual contains specific operational procedures related to the management of foreign national access to NASA facilities.

Additionally, as part of NASA's response to the January 2014 Focused Independent Security Review performed by NAPA, the Associate Administrator directed the Assistant Administrator for Protective Services on March 10, 2014, to establish a Foreign National Access Management (FNAM) Program, managed by the Office of Protective Services (OPS). The FNAM will seek to increase the effectiveness of NASA's existing procedures and implement improved procedures as required. Although OPS has the lead for the FNAM Program, OIIR will be engaged in the development and execution of the FNAM Program and will be the lead office in monitoring corrective actions as they relate to Export Control.

Estimated Completion Date: July 30, 2016.

Thank you for the opportunity to comment on the draft audit report. If you have any questions or require additional information, please contact David Flynn, NASA Headquarters Export Control Administrator, at 202-358-1792.



Michael F. O'Brien
Associate Administrator for
International and Interagency Relations

cc:
A/Administrator Bolden
A/Mr. Lightfoot
OPS/Mr. Mahaley
OIIR/Mr. Condes

National Aeronautics and Space Administration
 Office of the Administrator
 Washington, DC 20546-0001



February 7, 2014

ENCLOSURE 2

The Honorable Richard Thornburgh
 Chair
 Panel on Independent Review
 of NASA's Foreign National Access Management
 National Academy of Public Administration
 1600 K St., NW
 Suite 400
 Washington, DC 2006

Dear Governor Thornburgh:

I would like to take the opportunity to thank you and your National Academy of Public Administration panel for the thoughtful and thorough review of NASA's Foreign National Access Management program. I deeply appreciate the panel's overall recognition of NASA's need to balance the advancement of our missions--which are prescribed by statute and national policy to include significant and valuable international involvement--with the protection of our sensitive information and technologies. Your recognition of the professionalism of NASA employees and their on-going efforts to improve our security processes is also appreciated.

NASA is committed to reviewing your recommendations thoroughly and to having them inform changes to our existing processes. To that end, I have directed the appropriate NASA offices to examine each recommendation and, where appropriate, to incorporate the panel's recommendation into our processes or identify any barriers to implementation, including resource constraints. The panel identified several broad areas of interest, with associated findings and recommendations, which I have addressed below. I would also like to bring to your attention those areas where we do not fully concur with the panel's findings.

Integration of Foreign National Access Management

Across several findings, the Report recommends the need for a more integrated Foreign National Access Management program that consolidates and standardizes various components across multiple Agency offices. NASA recognizes the value of a consolidated program to provide clear, consistent, and effective direction concerning foreign national access management. I have asked the Assistant Administrator for Protective Services to work with relevant Headquarters offices and NASA Centers on how best to accomplish this integration, with an emphasis on: (1) providing consistent guidance, training, and oversight across all NASA Centers; (2) engaging all stakeholders in the identification of best practices and creation of operational manuals and materials; and (3) incorporating stronger compliance and accountability mechanisms into NASA's existing Integrated Center Functional Reviews.

Information Technology Security

The panel rightly identifies information technology (IT) security as a major area of emphasis. The panel's findings map with the findings of several other groups and reports, including by NASA's Inspector General, analyzing the state of IT security at NASA and across the Government as a whole. Based on these assessments, NASA's Chief Information Officer (CIO) is already moving to improve security in this area overall and the panel's findings will help to further inform these efforts. Specifically, the CIO will continue to work toward improvements in areas such as: (1) focusing IT security investments in capabilities that will provide a more holistic approach to protecting NASA's critical data; (2) developing a cross-functional IT Security and IT Operations project team to design and implement a modernized, risk-based solution for role-based elevated privileges management and tracking; and (3) implementing a more effective approval and maintenance paradigm that will enforce privilege pursuant to security requirements.

Counterintelligence

The panel identifies several areas in which NASA's counterintelligence process can be enhanced in terms of awareness, resources, and coordination. I recognize the need to elevate awareness of this important program across the Agency, as well as the benefits of an enhanced counterintelligence program with increased integration of Counterintelligence Special Agents into Center Operations. I have directed my Assistant Administrator for Protective Services to examine the report's findings in this area and to develop an educational and awareness program for the Agency. The Assistant Administrator has recognized and begun to address the need for additional resources, and I have also asked him to analyze the Panel's recommendation that NASA add assets in this area and to present his recommendations in the budget planning process.

While I appreciate the factors underlying the panel's suggestion that reporting of Special Agents be realigned to respective Center Directors, I concur with the panel's intent but not with the implementation recommendation. NASA's counterintelligence program is focused on Agency assets, and by retaining the existing reporting structure, we ensure a standardized and consistent program across the Agency. NASA believes the underlying factors for the panel's recommendation can be achieved with an increased focus on the relationship between counterintelligence personnel and their respective Center leadership teams, without eliminating the benefits of the current management approach.

Export Control

The panel found that NASA's export control processes could benefit from a more systemic and standardized approach, as well as by enhanced awareness of the program across the Agency. Accordingly, I have asked the Associate Administrator for International and Interagency Relations to review the panel's recommendations, with an emphasis on: (1) enhancing and standardizing our training and education for all Centers; and (2) exploring stronger compliance and accountability mechanisms. This review will include an assessment of additional resources that may be required to successfully implement the proposed recommendations.


Organizational and Functional Relationships

The panel made a number of observations and findings concerning communication, accountability, alignment, and awareness -- all Agency--level areas of emphasis to which I am strongly committed. I agree with the panel's focus on the importance of senior leadership attention and cross-Agency cooperation to ensure an increasingly effective security program. As you know, I am committed to our continuous improvement in this area, including by requesting this independent assessment of our operations. I will direct all NASA senior leadership to review this important report and, as appropriate, they will be involved in the examination and execution of the above-identified actions. I will also direct all senior leadership to express regularly to the workforce that security and the appropriate management of foreign national access to our facilities, technology, and information are critical elements to the successful implementation of our mission.

Relative to the panel's general findings regarding NASA's culture, specifically about Center competition and the panel's suggestion that NASA may have a tendency not to be a "learning culture," I would share my view that NASA's culture combines the richness of diversity and appropriately healthy competition among our Centers, while fostering an overall NASA team environment. I think that the panel understands NASA's commitment to this balance. Of course, we must still ensure better consistency, alignment, and accountability among all elements of NASA. As a former astronaut and leader in NASA's independent safety oversight panel, I have seen NASA continue to grow and learn from its past triumphs and tragedies. I expect no less in this area.

I want to thank you and the panel again for a job well done. The panel's acute level of attention to the details of foreign national access management, while recognizing the unique role and importance of international engagement to NASA's mission, ensures that this Report will make an essential contribution to the Agency's efforts as we continue to move forward to open frontiers, reach new heights, partner with international entities to advance our understanding of the world, and protect the Nation's investment in our research, technology, and programs.

Sincerely,



Charles F. Bolden, Jr.
Administrator

cc:
Joseph P. Mitchell, NAPA Director of Project Develop
Joe Thompson, NAPA Project Director

Biography of Mr. Richard Keegan

Richard Keegan was appointed as NASA's Associate Administrator for Mission Support on August 11, 2013. The Mission Support Directorate enables program and institutional capabilities to conduct NASA's aeronautics and space activities. As the directorate's associate administrator, Keegan is responsible for most NASA management operations, including human capital management, strategic infrastructure, procurement, protective services, headquarters operations, the NASA Shared Services Center, cross-agency support, and construction and environmental compliance and restoration.

Mr. Keegan also serves as NASA's Associate Deputy Administrator, a role he has fulfilled since December, 2010. In this role, he assists NASA's Deputy Administrator and Administrator in day-to-day agency operations, across the broad scope of institutional and workforce issues, and with contingency and continuity of operations planning. Previously, Keegan served as Deputy Associate Administrator of the Mission Support Directorate since its creation in April, 2010. For the prior four years he was Director of NASA's Office of Program and Institutional Integration. In those roles, he served as the focal point for balancing priorities for mission directorates, mission support offices and field centers for the agency.



Since coming to NASA Headquarters in 2002, Keegan has served in senior business management positions in mission directorate and mission support offices. He also worked in a variety of jobs during 21 years at NASA's Goddard Space Flight Center in Greenbelt, Md., NASA Headquarters and the Department of Energy. He began his Federal service in June, 1980. Prior to that, he was a junior high school science teacher for two years. He has degrees in biological sciences and secondary education from the University of Maryland.

Chairman PALAZZO. Thank you, Mr. Keegan.
I now recognize our next witness, Ms. Martin.

**TESTIMONY OF MS. BELVA MARTIN, DIRECTOR,
ACQUISITION AND SOURCING MANAGEMENT,
GOVERNMENT ACCOUNTABILITY OFFICE**

Ms. MARTIN. Thank you, Chairmen Palazzo, Broun, and Ranking Member Maffei, and Members of the Subcommittee for this opportunity to participate in this hearing. I will summarize my written testimony and ask that the entire statement be placed in the record.

Mr. Keegan has summarized actions that NASA is taking or plans to take to address recommendations from GAO, the IG, and NAPA. GAO issued its report in April. Today, I will focus on one area: developing a risk-based approach to compliance where NASA can leverage existing resources to make improvements that can help it to effectively balance its mission of protecting sensitive technologies and information and supporting international agreements on the one hand and disseminating important scientific information as broadly as possible.

But in order to develop a risk-based approach, NASA needs to know where technologies it is trying to protect and where they are located. We found that NASA headquarters officials and some of the front-line managers, the Center Export Administrators, or the CEAs, lack a comprehensive inventory of the types and locations of export-controlled technologies at the centers, severely limiting their ability to identify and internal and external risks to compliance. This is not a new issue. The NASA IG identified this issue as early as 1999.

While acknowledging the benefits of obtaining comprehensive knowledge of export-controlled technologies, NASA headquarters officials state that doing so is resource-intensive. But as I have just stated, NASA has an opportunity to leverage existing resources. So absent a NASA-wide initiative, three centers began recent efforts to identify export-controlled technologies at their centers. At one of these centers the Counterintelligence Office collaborated with the CEA to identify the most sensitive technologies and develop protective measures. This is one example of a risk-based approach that could be implemented NASA-wide to enable NASA to target resources to first identify the most sensitive technologies and then ensure the location of these are known to staff and are protected. NASA concurred with our recommendations in this area.

As I mentioned, the export-control—I am sorry, the Export Center Administrators are the front-line managers. These professionals are responsible for ensuring that all center program activities comply with U.S. export control laws and regulations. However, our review found wide variations across the centers in position and resource allocation for these professionals.

For example, seven of ten CEAs are at least three levels removed from the center director. We were told by some CEAs that such placement makes it difficult to maintain authority and visibility to staff and to obtain the resources necessary to carry out their responsibilities. We found variations among centers and resource allocation and in particular found indications that the resources as-

signed to export controls at centers did not always appear to be commensurate with the export control workload. NASA concurred with our recommendations to define the appropriate level and placement for the CEA function and to assess workload to determine appropriate resources needed at each center.

In closing, ensuring compliance with export controls is important because just one instance of unapproved foreign national access to NASA information or unapproved release of scientific and technical information increases the risk of harm to national security. Therefore, it is important that NASA leverage existing resources to identify export control items and assess vulnerabilities in adopting a risk-based approach to ensuring compliance. Effective oversight is also important to ensure consistent adherence across NASA centers. Moreover, it will be important for NASA to be vigilant in assessing actions taken to help ensure effective implementation and to avoid a relapse into former practices. Unless this is done, NASA will remain at risk of unauthorized access to its export-controlled technologies.

Mr. Chairman, Ranking Members, this concludes my oral statement. I will be happy to address any questions you may have. Thank you.

[The prepared statement of Ms. Martin follows:]

United States Government Accountability Office



Testimony

Before the Subcommittees on
Space and Oversight, Committee
on Space, Science, and Technology,
House of Representatives

For Release on Delivery
Expected at time, 10:00 a.m. ET
Friday, June 20, 2014

EXPORT CONTROLS

NASA Management
Action and Improved
Oversight Needed to
Reduce the Risk of
Unauthorized Access
to Its Technologies

Statement of Belva Martin, Director,
Acquisition and Sourcing Management

Chairmen Palazzo, Broun, Ranking Members Edwards, Maffei, and Members of the Subcommittees:

Thank you for the opportunity to participate in today's hearing on the National Aeronautics and Space Administration's (NASA) system to protect sensitive information, including through its export control program. NASA develops new and sophisticated technologies to accomplish its missions in areas such as robotic probes to explore the surface of Mars and spacecraft to transport humans and cargo beyond low-earth orbit. The National Aeronautics and Space Act directs NASA to provide the widest practical and appropriate dissemination of information concerning its activities and results. The U.S. export control system, regulated primarily by two agencies—the Departments of State and Commerce—seeks to limit the risk of sensitive information and items falling into the wrong hands while allowing legitimate sharing of information and trade to occur.¹ U.S. export control regulations require any exporter, including NASA, to protect its sensitive information and technology. To effectively achieve its mission, NASA has to strike a balance between protecting sensitive technologies and information and preserving its mission to support international partnerships and dissemination of information. NASA's export control program is governed by a NASA Policy Directive and NASA Procedural Requirement (export control NPR). These policies outline the goals of the export control program and NASA export control procedures contain detailed requirements and responsibilities for implementing the policy. NASA performs its mission through numerous programs and projects across its 10 research and space centers and headquarters.² NASA Headquarters Export Administrator (HEA), the

¹ Generally, exporters may submit an export license application to State if their items are controlled on the International Traffic in Arms Regulations (ITAR) U.S. Munitions List or to Commerce if their items are controlled on the Export Administration Regulations (EAR) Commerce Control List. Both the ITAR and EAR provide for exemptions and exceptions to licensing requirements, respectively. See 22 C.F.R. Part 12 and 15 C.F.R. Part 740. The Export Administration Act is not permanent legislation. Authority granted under the act lapsed in August 2001, 50 U.S.C. App. § 2419. However, Executive Order No. 13222, Continuation of Export Control Regulations, which was issued in August 2001 under the authority provided by the International Emergency Economic Powers Act (50 U.S.C. §§ 1701-1707) continues the controls established under the act, and the implementing Export Administration Regulations. Executive Order No. 13222 requires an annual extension and was recently renewed by Presidential Notice on August 8, 2013. 78 Fed. Reg. 49,107 (Aug. 12, 2013).

² The Jet Propulsion Laboratory (JPL) is a NASA federally funded research and development center managed by the California Institute of Technology under contract with NASA. For purposes of this statement, we refer to JPL as a NASA center.

Center Directors, and their appointed Center Export Administrators (CEA), as well as Center Project Managers are some of the key personnel responsible for implementing NASA's export control program.

Allegations of export control violations at two NASA centers over the last two years have raised questions about NASA's ability to protect its sensitive technologies. In April 2014, we issued a report entitled *Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the Risk of Unauthorized Access to Its Technologies*.³ My remarks today are based on this report and initial actions NASA reported it has taken to begin addressing our recommendations.

Like the April 2014 report, this statement discusses (1) NASA's export control policies and how centers implement them, and (2) the extent to which NASA Headquarters and CEAs apply oversight of center compliance with its export control policies.

For our April 2014 report, we reviewed export control laws and regulations, NASA export control policies, and State and Commerce export control compliance program guidance. We also reviewed NASA information on foreign national visits and technical papers and interviewed export control and security officials from NASA Headquarters and its 10 centers as well as from other agencies. Our work was performed in accordance with generally accepted government auditing standards.

Weaknesses in Implementation of NASA Export Control Procedures Create Export Control Vulnerabilities

We found weaknesses in the implementation of NASA's export control policy and procedures concerning the CEA function and foreign national access procedures, which increase the risk of unauthorized access to export-controlled technology.

Variations in CEA Position, Function, and Resources: NASA's export control policy provides the CEA the responsibility to ensure compliance of all Center program activities with U.S. export control laws and regulations and states that the position should be "senior-level," but does not define what "senior-level" means. NASA headquarters export control officials define senior-level as a person at the GS-15 level or in the senior

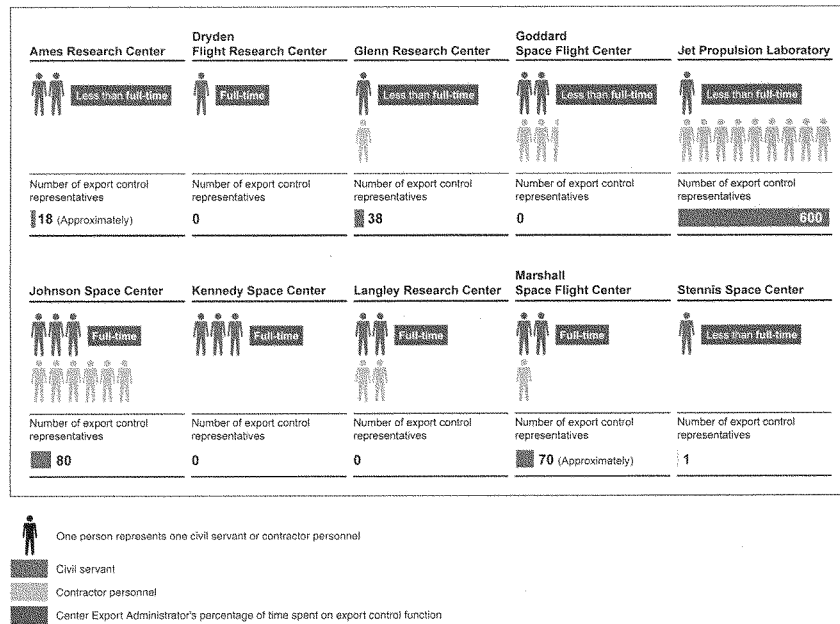
³ GAO-14-315 (Washington, D.C.: April 15, 2014).

executive service; however, we found that no CEAs were at the senior executive service level, three were GS-15s, and the CEAs at the remaining seven centers were at the GS-14 and GS-13 levels.

In addition, NASA's export control NPR does not contain a provision on the placement of the export control function and CEA within the center's organizational structure. At some centers where they were several levels removed from the Center Director, CEAs stated that this placement makes it difficult to maintain authority and visibility to staff, to communicate concerns to center management, and to obtain the resources necessary to carry out their export control responsibilities. Conversely, a CEA at another center stated that his placement as Special Assistant to the Center Director creates a supportive environment to incorporate export controls into the project management processes and to require and provide export control training for the majority of center staff.

NASA headquarters' export control officials, as well as several CEAs, noted that limitations in staff resources and time spent on export control functions makes it difficult to carry out the full range of export control duties, such as improving center export control procedures or providing a more robust export control training program. However, NASA's export control NPR does not discuss the allocation of resources for the export control function or for the CEA within the center, and, according to NASA headquarters' export control officials, each Center Director has the discretion of how to allocate resources to the export control function. As a result, we found variation among the centers in the staff resources assigned to the export control function, as shown in figure 1.

Figure 1: NASA Center Export Control Staff Resources (as of Fiscal Year 2013)



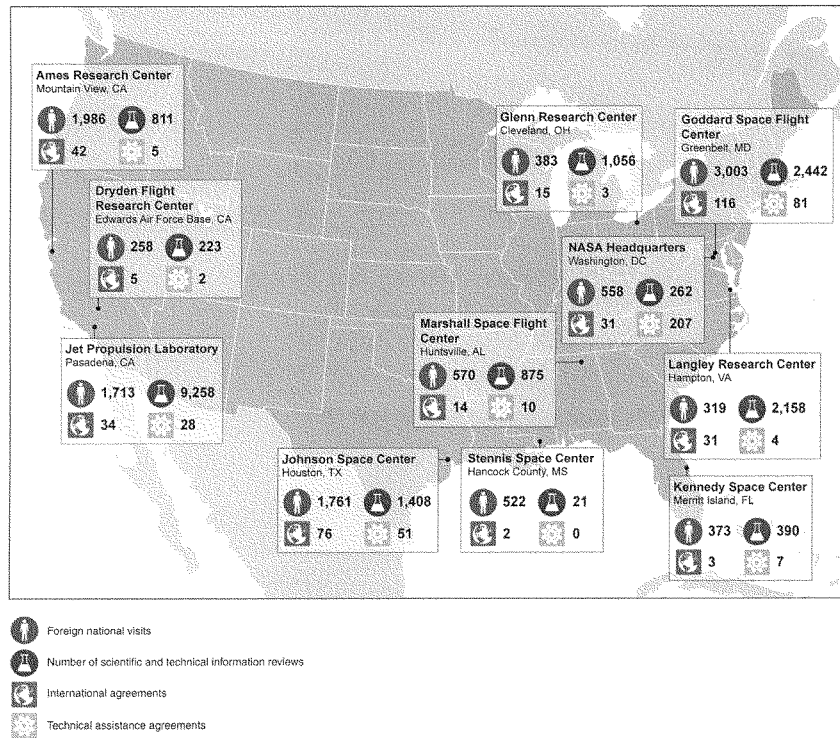
Source: GAO analysis of NASA data. | GAO-14-690T

Moreover, we found indications that the resources assigned to export controls at centers did not always appear to be commensurate with the export control workload. Specifically, 8 of the 10 centers had two or fewer civil servant staff to carry out export control activities for hundreds to thousands of foreign national visits, Scientific and Technical Information (STI) reviews, international agreements, and technical assistance agreements. For example, at one center in 2013, two civilian export

control officials working less than full time on export control activities were responsible for reviewing and providing any needed export control access restrictions for over 3,000 foreign national visitors and conducting STI reviews for over 2,000 publications. NASA's procedural requirements for STI requires that all STI intended for release outside of NASA or presented at internal meetings where foreign persons may be present undergo technical, legal, and export control reviews, among others, to ensure that information is not unintentionally released through publication.⁴ See figure 2 for export control workload by center for fiscal year 2013. The CEA at one of the centers stated that the time to complete required review activities leaves little time to improve procedures or provide more robust training. To address the variations in authority, placement, and resources of the CEAs, we recommended NASA establish guidance defining the appropriate level and placement for the CEA function and assess the CEA workload to determine appropriate resources needed at each Center. NASA concurred, indicating plans to update existing guidance and to explore strategies to enhance support for the export control function.

⁴NASA NPR 2200.2C, "Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information," STI NPR. (Apr. 19, 2001)

Figure 2: CEA Export Control Workload Activities in Fiscal Year 2013



Weaknesses in Foreign National Access: Throughout fiscal year 2013 NASA centers and Headquarters approved over 11,000 foreign national visits for periods ranging from less than 30 days to greater than 6 months. NASA's security procedure requires screening of all foreign national visitors prior to gaining approval for access to any NASA facility. However, we identified instances in which NASA security procedures for foreign national access were not followed, which were significant given the potential impact on national security or foreign policy from unauthorized access to NASA technologies. Specifically, at one center, export control officials' statements and our review of documentation identified instances between March and July of 2013, where foreign nationals fulfilled the role of sponsors for other foreign nationals by identifying the access rights to NASA technology for themselves and other foreign nationals for one NASA program.⁵ This is not in compliance with NASA's security procedures which provide that only NASA civil servants or JPL employees who are U.S. citizens can act as sponsors for foreign nationals, which is one step in NASA's process of approving and activating foreign national access. This center is taking action to address this issue and, as of December 2013, it developed a new approval process and criteria for foreign nationals requesting access to center automated databases and made revisions to center policies for information systems and foreign national access. We identified planned corrective actions at this and other Centers related to the management of foreign national access and, in our April report, we recommended that NASA develop plans with specific time frames to monitor these corrective actions to ensure their effectiveness. NASA concurred and indicated that it plans to take action to increase the effectiveness of its existing procedures and implement improvements.

⁵ A foreign national sponsor is typically a NASA Project Manager or other NASA official who establishes and endorses the need for a relationship between the foreign national and NASA and requests their access to NASA facilities and information technology systems by identifying the foreign national's access rights to NASA technology for a NASA program.

NASA Lacks a Comprehensive Inventory of Export-Controlled Technologies and Is Not Fully Utilizing Oversight Tools

We found that NASA headquarters export control officials and some CEAs faced challenges in providing effective oversight. In particular, the lack of a comprehensive inventory of export-controlled technologies and not effectively utilizing available oversight tools limit their ability to identify and address risks.

Lack of a Comprehensive Inventory of Export-Controlled Technologies: NASA headquarters export control officials and CEAs lack a comprehensive inventory of the types and location of export-controlled technologies at the centers, limiting their ability to identify internal and external risks to export control compliance. Five CEAs told us that they do not know the types and locations of export-controlled technologies, but rather rely on NASA program and project managers to have knowledge of this information. NASA's export control NPR provides that NASA Center Program and Project Managers, in collaboration with CEAs, are to identify and assess export-controlled technical data. Additionally, NASA Center Project Managers are required by NASA's export control NPR to provide appropriate safeguards to ensure export-controlled items⁶ and technical data are marked or identified prior to authorized transfer to foreign parties consistent with export control requirements. The CEA and security chief at one center told us that they requested a plan identifying where export-controlled and sensitive technologies are located within a research branch in order to facilitate foreign national visit requests. According to the branch manager, he was unable to provide this information, stating it would be too cumbersome to map out all of that information and try to restrict access to the areas with sensitive technologies. Assessing areas of vulnerability, including identifying and assessing export-controlled items, could better ensure that consistent procedures are practiced. NASA's lack of a comprehensive inventory of its export-controlled technologies is a longstanding issue that the NASA Inspector General identified as early as 1999.⁷

Three centers began recent efforts to identify export-controlled technologies at their centers—one of which involves coordination with the center counterintelligence officer. Specifically, at this center, the

⁶ "Item" means commodities, software, and/or technology/technical data. NASA NPR 2190.1B, "NASA Export Control Program" (Dec. 27, 2011).

⁷ NASA Inspector General Report, *NASA Control of Export-Controlled Technologies*, IG-99-020, (Mar. 31, 1999).

counterintelligence office collaborated with the CEA to conduct a sensitive technology survey—designed to identify the most sensitive technologies at the center—to better manage risks by developing protective measures for these technologies in the areas of counterintelligence, information technology security, and export controls. Such approaches, implemented NASA-wide, could enable the agency to take a more risk-based approach to oversight by targeting existing resources to identify the most sensitive technologies and then ensure the location of such technologies are known and protected. To implement a risk-based approach, we recommended NASA build off of existing information sources, such as assessments by NASA's counterintelligence office, to identify targeted technologies. In its response, NASA highlighted plans to implement a risk-based approach that would include CEAs, program managers, and counterintelligence officials.

Underutilization of Oversight Tools: NASA's oversight tools, including annual audits, export control conferences with CEA, and voluntary disclosures, have identified deficiencies, but NASA headquarters has not addressed them. Specifically, we found that seven centers have unresolved findings, recommendations, or observations spanning a period from 2005 to 2012, in areas including export control awareness, management commitment, resources, training, foreign national visitor processes, and disposal of property. At five centers, responding to audit findings and implementing recommendations required that the CEA coordinate with other offices and programs across the center beyond the CEA's control. The remaining two centers cited resource constraints, organizational priorities, and insufficient coordination with center management as barriers to implementing corrective actions and resolving recommendations. NASA's current procedures do not address coordination among offices at a center to address findings from annual audits.

Further, NASA headquarters export control officials hold annual export control program reviews with the CEAs to discuss export control changes and CEA concerns and recommendations for the program. At NASA's 2013 annual review, the CEAs presented NASA headquarters export control officials with a list of comments regarding the export control program, many of which echo the issues raised in our April 2014 report, such as CEA position and resources, foreign national access, and awareness of export-controlled technologies. NASA headquarters' export control officials stated that they agree with the issues raised by the CEAs but acknowledged that they have not fully addressed the CEA concerns from the most recent program review in March 2013 and have not

developed specific plans to do so. In fact, we found that over the last 3 years, NASA headquarters export control officials provided only one policy update or other direction to address export control concerns raised by the CEAs. In our April report, we made two recommendations to address underutilization of the audit and program review tools. To ensure implementation of audit findings, we recommended that NASA direct Center Directors to oversee implementation of the audit findings. Similarly, we recommended that NASA develop a plan, including timeframes, to ensure CEA issues and suggestions for improvement are addressed. NASA concurred and plans to revise existing guidance.

NASA may also be missing an opportunity to use voluntary disclosures to help improve export control compliance. NASA's export control NPR provides that it is every NASA employee's personal responsibility to comply with U.S. export control laws and regulations; and further provides the Departments of State and Commerce's regulatory requirements for voluntary self disclosure of noncompliance in export activities, even if the errors were inadvertent. NASA's headquarters' export control program officials told us that few or no voluntary disclosures might indicate a weakness in a center's export control program. We found little usage of the voluntary disclosure process at the NASA centers: a total of 13 voluntary disclosures divided among four of the NASA centers since 2011, and potential noncompliance ranged from failure to file a record of shipment to Germany to potential foreign national exposure to a program's technical data. The remaining six NASA centers have not submitted voluntary disclosures since 2011. We found that a similar event may lead to a voluntary disclosure at one center but not another and that CEA approaches toward voluntary disclosures at some centers may affect NASA's ability to identify and report potential violations of export control regulations. To ensure consistency in reporting potential export control violations, in our April 2014 report, we recommended that NASA re-emphasize to CEAs the requirements on how and when to notify headquarters. NASA concurred and plans to revise and develop additional guidance.

As stated above, NASA concurred with all of our recommendations and stated that our findings and recommendations complement results from the recent reviews by the NASA's Inspector General and the National Academy of Public Administration. Further, NASA stated in its response to each of these reviews that it plans to adopt a more comprehensive, risk-based approach to enhance its export control program.

Subsequent to our report, the NASA Administrator issued an email to all employees reiterating the importance of the export control program and announcing plans to expand the online and in-person export control training. This is an important step as it sets a tone from the top and could help ensure the centers apply consistent approaches. However, it will be important for NASA to be vigilant in assessing actions taken to help ensure effective implementation and to avoid a relapse into the former practices. Collectively, improvements in all of these areas can help NASA strike an effective balance between protecting the sensitive export-controlled technologies and information it creates and uses and supporting international partners and disseminating important scientific information as broadly as possible.

Mr. Chairmen, Ranking Members, and members of the subcommittees, this concludes my prepared remarks. I would happy to answer any questions that you may have.

**GAO Contact and
Staff
Acknowledgements**

For questions about this statement, please contact Belva Martin at (202) 512-4841, or at martinb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony include William Russell, Assistant Director; Caryn Kuebler, Analyst-in-Charge; Marie Ahearn; Lisa Gardner; Laura Greifner; Amanda Parker; and Roxanna Sun.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548



Please Print on Recycled Paper.

Belva M. Martin

Since August 2009, Belva Martin has been a Senior Executive serving as a Director in the Acquisition and Sourcing Management team at GAO. In this role, she manages a varied portfolio of programs reviewing export control, the defense supplier base, Army modernization, defense and civilian acquisition workforce, and various contracting issues. Prior to assuming this position, from 2003-2009, Ms. Martin served as an Assistant Director managing reviews of federal human capital, EEO, diversity, and redress issues. She also directed reviews of issues related to recruiting and retaining experienced, older federal workers; efforts to identify factors influencing Hispanic representation in the federal government; and issues related to reemployment rights of uniformed servicemembers. From 1993 to 2003, she managed a portfolio of issues related to the Federal Aviation Administration including the National Airspace System modernization program, aviation finance, and FAA organization and management. In all of these roles, she produced numerous written reports and oral briefing for Hill clients and testified several times as a GAO witness.

Her federal career spans 36 years—35 with GAO. Ms. Martin received her undergraduate degree in Political Science/Public Administration from South Carolina State University and a Masters degree in Political Science from Howard University.

She is the recipient of numerous GAO-wide awards, including two of agency's highest—the Distinguished Service Award and the Meritorious Service Award (twice)—the Excellence in Human Capital Award, and the Equal Employment Opportunity Award, in addition to numerous team-based awards.

She presently resides in Mitchellville, MD with her husband John; they have two young adult children.

Chairman PALAZZO. Thank you, Ms. Martin.
I now recognize our next witness, Ms. Robinson.

**TESTIMONY OF MS. GAIL A. ROBINSON,
DEPUTY INSPECTOR GENERAL,
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION**

Ms. ROBINSON. Thank you, Mr. Chairman, Members of the Subcommittee. Thank you for the opportunity to testify today about our work examining NASA's management of foreign national access, compliance with export control laws, and related security issues.

As you mentioned, in January of each year the OIG submits to the House and Senate Appropriations Committees a letter describing the audits and investigations we conducted the preceding year that shed light on the extent to which NASA is complying with Federal export control laws. In our most recent letter we cited four audits examining security controls for NASA's information technology assets, many of which contain data subject to export control laws; and also a special review examining a Chinese national's access to Langley Research Center, which has also been mentioned.

Subsequent to that letter, we also completed our review involving foreign national access and export control issues at Ames. I summarized those reviews in my written testimony and also described several of our audits.

In my oral statement, I would like to highlight several themes from our oversight work that echo findings that the GAO and NAPA made as well. First, our work leads us to conclude that NASA needs to take a more standardized and systematic approach to its management of both foreign national access and export control. In the Langley matter, we were struck by the highly bureaucratic nature of NASA's process for reviewing foreign visit requests. For example, we noted that many individuals involved in the process appeared to view their roles in isolation with little consideration or understanding of the role played by others.

Similarly, in the Ames review we found a lack of early coordination between project and export control personnel as well as deep disagreement between those groups regarding whether work performed by foreign nationals involved export-controlled technology. Indeed, the issue only surfaced when the Ames scientists sought to publish a paper many months after work on the project had begun. In addition, it appeared that NASA lacked an efficient mechanism to resolve the dispute. We believe that NASA needs to work towards a model that encourages agency scientists and engineers to consult with export control professionals when projects involving foreign nationals are initiated and develop a mechanism for resolving disputes in a timely manner.

Second, we believe export control professionals at the various NASA Centers should improve their understanding of the type and location of export-controlled technology and information at their Centers and at other facilities under their control. For example, in the course of a recent investigation we learned that a Center Export Control Administrator was not aware that an off-site lab under his responsibility contained export-controlled equipment and

data. Center export control personnel need this information to ensure that foreign nationals do not have access to those areas.

Third, we encourage NASA to study the best practices noted in the GAO and NAPA reports and adopt them at all of their Centers. As we have learned through our oversight work in other areas, NASA Centers often work independently from one another and do not consistently learn about or benefit from successful practices developed at other locations. We were particularly intrigued by the discussion about the Jet Propulsion Laboratory's success with using engineers and scientists as Export Control Representatives to work with the Lab's export control staff, a model that could help address the lack early interaction between project managers and export control staff we observed at Ames as well as provide a mechanism for dispute resolution.

Finally, we agree that NASA needs to improve and expand training to provide its scientists and engineers with a deeper understanding of the importance of complying with the rules and regulations governing export control and foreign national access.

That concludes my remarks and I would be pleased to answer any questions. Thank you.

[The prepared statement of Ms. Robinson follows:]

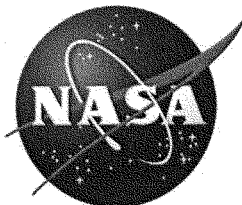
Testimony before the Subcommittee on Space
Committee on Science, Space, and Technology

United States House of Representatives

For Release on Delivery
expected at 10:00 a.m.
on June 20, 2014

NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information

Statement of
Gail A. Robinson
Deputy Inspector General
National Aeronautics and Space Administration



Mr. Chairmen, Ranking Members, and Members of the Subcommittees on Space and Oversight:

The Office of Inspector General (OIG) is committed to providing independent, aggressive, and objective oversight of NASA programs and personnel, and we thank you for inviting us to discuss our work relating to the Agency's management of foreign national access to its information and Centers, compliance with export control laws, and related security issues.

In January of each year, the OIG submits to the House of Representatives and Senate Appropriations Committees a letter describing the audits and investigations we conducted the preceding year that shed light on the extent to which NASA is complying with Federal export control laws.

In our most recent letter we summarized

- four audits examining security controls for NASA's information technology (IT) assets, many of which contain data subject to export control laws; and
- a special review examining a Chinese national's access to the Langley Research Center (Langley) in Hampton, Virginia.

Before highlighting two of the audits and describing the Langley investigation and another special review involving foreign nationals and export issues at the Ames Research Center (Ames) in Mountain View, California, I will highlight several themes from our oversight work that echo findings made by the Government Accountability Office (GAO) and the National Academy of Public Administration (NAPA) in their recent examinations of export control practices and management of foreign national access at NASA.¹

First, our audit and investigative work lead us to conclude that NASA needs to take a more standardized and systematic approach to both foreign national access and export control management. In the Langley matter, we were struck by the highly bureaucratic nature of NASA's process for reviewing foreign visit requests. For example, we noted that the many individuals involved in the process appeared to view their roles in isolation, with little consideration or understanding of the role played by others. Similarly, in the Ames review, we encountered a lack of early coordination between project and export control personnel, as well as deep disagreement between these two groups regarding whether work performed by foreign nationals involved technology subject to the International Traffic in Arms Regulations (ITAR) that control the transfer of military and space-related technology. Indeed, the issue only surfaced when the Ames scientists sought to publish a paper many months after work on the project had begun. In addition, it appeared that NASA lacked an efficient mechanism to resolve the dispute between the two groups, which dragged on for months. We believe that NASA needs to work toward a model that

¹ GAO, "Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the risk of Unauthorized Access to its Technologies" (GAO-14-315, April 2014); and NAPA, "An Independent Review of Foreign National Access Management" (January 2014).

encourages Agency scientists and engineers to consult with export professionals when projects involving foreign nationals are initiated and develop a mechanism for resolving disputes in a timely manner.

Second, we believe export control professionals at the various NASA Centers could improve their understanding of the type and location of export-controlled technology and information at their Centers and other facilities under their Center's control. For example, over the course of a recent investigation, we learned that a Center Export Control Administrator was not aware that an off-site lab under his responsibility contained export-controlled equipment and data. Center export control personnel need this type of information to ensure that foreign nationals do not have access to these areas.

Third, we encourage NASA to study the best practices noted in the GAO and NAPA reports and adopt them at all its field Centers. As we have learned through our oversight work in other areas, NASA Centers often work independently from one another and do not consistently learn about or benefit from successful practices developed at other locations. We are particularly intrigued by discussion in the GAO report about the Jet Propulsion Laboratory's (JPL) success with using engineers and scientists as export control representatives to work with the JPL's export control staff – a model that could help address the lack of early interaction between project managers and export control staff we observed at Ames as well as provide a mechanism for dispute resolution.

Finally, we agree that NASA needs to improve and expand training to provide its scientists and engineers with a deeper understanding of the importance of complying with rules and regulations governing export control and foreign national access.

As noted above, NASA stores export-controlled information in various Agency databases. We have repeatedly reported that ensuring the security of its information and IT systems remains one of NASA's top management challenges. On the one hand, the Agency's mission to widely disseminate and publicly share its information helps push the boundaries of science and space exploration; however, at the same time, the Agency must ensure the security of its IT assets and comply with an array of complex export control laws and regulations. Below, I summarize several of our recent audit and investigative work products that involve IT security, foreign national access, and export control issues.

In a June 2013 audit report, we examined whether NASA's IT governance structure – its process for designing, procuring, and protecting IT resources – appropriately aligns authority and responsibility to support the Agency's overall mission.² We found that the decentralized nature of NASA's operations and the Agency's longstanding culture of autonomy hinder its ability to implement effective IT governance. NASA's Chief Information Officer (CIO) has limited visibility and control over a majority of the Agency's IT investments, operates in an organizational structure that marginalizes the authority of the position, and cannot enforce security measures

² NASA OIG, "NASA's Information Technology Governance" (IG-13-015, June 5, 2013).

across NASA's computer networks. Specifically, although the CIO is responsible for developing IT security policies and implementing an Agency-wide IT security program, the position lacks authority and control over the majority of NASA's networks and therefore the CIO is unable to enforce implementation of IT security programs across all Agency IT assets.

We made eight recommendations to the CIO to overcome the barriers that have resulted in inefficient and ineffective management of the Agency's IT assets and security. Effective implementation of these recommendations will require a cultural shift and significant changes to the Agency's IT management decision-making regime, including the realignment of authority and responsibilities. To date, NASA is taking appropriate steps to meet our recommendations.

In a separate audit, we examined NASA's procedures related to its acquisition of IT security assessment and monitoring tools.³ NASA spends more than \$1.5 billion annually on its IT assets, including approximately 550 information systems the Agency uses to control spacecraft, collect and process scientific data, provide security for Agency IT infrastructure, and enable personnel to collaborate with colleagues around the world. However, the Agency's use of advanced technology, coupled with the large size of its internet-accessible networks, makes NASA an attractive target to cyber attacks. To thwart such attacks, NASA must ensure that Agency IT systems are regularly safeguarded, assessed, and monitored.

We found that the Agency has not fully implemented a process for identifying its IT security assets despite spending at least \$58 million annually on IT security, a portion of which is used to acquire and manage security assessment and monitoring tools. Because NASA does not have a process that captures, consolidates, and assesses IT security tool requirements across the Agency, centralized purchases of such tools do not regularly occur. This inability limits NASA's efforts to reduce cost and improve program efficiencies on critical IT investments. To improve NASA's process for acquiring Agency-wide IT security assessment and monitoring tools, we made four recommendations to which Agency management concurred and proposed appropriate corrective actions.

In addition to our audit work, we also dedicate significant resources to investigating IT and other security-related issues. Of the 263 active cases currently being handled by our Office of Investigations, 56 involve cyber intrusions and misuse of NASA IT equipment and 15 involve allegations of export control violations. In one recently concluded investigation, we found that insufficient security practices at a facility located on the campus of one of NASA's university partners allowed unauthorized foreign nationals to enter a laboratory containing export-controlled equipment and data. Although the foreign nationals denied copying any data from the lab and a later search of their electronic media failed to uncover any controlled information, we were unable to definitively exclude that possibility. In addition, two of our most high-profile investigations

³ NASA OIG, "NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools" (IG-13-006, March 18, 2013).

during the past year examined foreign national access and export control issues. I summarize each of these investigations below.

Chinese National's Access to Langley

In March 2013, Bo Jiang, a Chinese national working as a NASA contractor at Langley, was returning to China when Department of Homeland Security (DHS) agents searched him at Dulles International Airport as part of an investigation of potential export control violations. After questioning him about the electronic media in his possession, agents took Jiang into custody and charged him with making a false statement to Federal authorities because a search of his belongings revealed media he had not declared. After more than 6 weeks in detention, Jiang pleaded guilty to a misdemeanor security offense and left the country. Subsequent to the plea, the OIG opened an administrative investigation to examine the process by which Jiang came to work at Langley and the information and IT resources to which he had access.

Jiang originally came to the United States in 2007 as a Ph.D. student at Old Dominion University and began working at Langley in January 2011 under a contract with the National Institute of Aerospace. In November 2011 and again in November 2012, Jiang visited family in China and took with him a NASA-provided laptop computer. During the second visit, Langley export control officials raised concerns about Jiang's travel and access to NASA information.

We found that even though Langley's process for requesting access for foreign nationals was structured pursuant to NASA regulations, it was overly complex and not sufficiently integrated to ensure that responsible personnel had access to all relevant information. In addition, we determined that several employees who had roles in the screening process made errors that contributed to the confusion about the proper scope of Jiang's access to Langley facilities and IT resources. We made six recommendations to improve NASA's foreign visitor approval process, and NASA concurred with each.⁴

In the wake of the Jiang incident, Langley management has taken steps to strengthen its foreign national access process, including increased education and training for Langley employees, revising the form used to request access for foreign nationals, and ensuring the Center CIO's office is involved in the foreign visitor request process.

Ames ITAR investigation

Beginning in 2009, Federal law enforcement agencies received complaints that foreign nationals working as contractors at Ames had been given improper access to information subject to ITAR. These complaints led to a 4-year criminal investigation by the Federal Bureau of Investigation, Department of Homeland Security, and OIG. In February 2013, the U.S. Attorney for the Northern District of California closed the case without bringing criminal charges, and the OIG continued to

⁴ NASA OIG, "Bo Jiang's Access to NASA's Langley Research Center" (October 22, 2013).

investigate the allegations as an administrative matter. In February 2014, we provided a 41-page report outlining our investigation and findings to the NASA Administrator. While the full report could not be released publicly because it contains information protected by the Privacy Act of 1974, we provided copies to several Congressional committees and posted a public summary on our website.⁵

Although we did not find intentional misconduct by any Ames civil servants, we believe several Ames managers exercised poor judgment in their dealings with foreign nationals. With respect to ITAR issues, we found that several foreign nationals without the required licenses worked on projects that were later determined to involve ITAR-restricted information. In addition, on two occasions a senior Ames manager inappropriately shared documents with unlicensed foreign nationals that contained ITAR markings or had been identified as containing ITAR-restricted information by NASA export control personnel. However, we also found significant disagreement between scientists and engineers at Ames and export control personnel at the Center and NASA Headquarters as to whether the work performed by foreign nationals involved ITAR-controlled technology. Moreover, the foreign nationals subsequently applied for and received licenses permitting them to access the information. We concluded that these incidents resulted more from carelessness and a genuine disagreement about whether the information qualified for ITAR protection than an intentional effort to bypass ITAR restrictions.

We also found that a foreign national working at Ames inappropriately traveled overseas with a NASA-issued laptop containing ITAR-restricted information. Even though the foreign national had an ITAR license at the time, the regulations forbid taking export-controlled information out of the country. However, we were unable to substantiate concerns that the foreign national shared controlled information while overseas. Further, we found that security rules designed to protect NASA property and data were not consistently followed in a rush to bring foreign nationals on board at Ames. For example, contrary to NASA rules a foreign national improperly received unescorted access privileges to Ames in 2006 prior to the completion of required background checks and worked at the Center for nearly 3 years without a required security plan.

Finally, we uncovered no evidence to support allegations that any foreign nationals at Ames were provided classified information during the period covered by our review. We encouraged NASA to consider the findings in our Ames report together with the NAPA review and previous OIG reports as it refines its foreign national and export control programs.

In closing, we are encouraged that NASA has embraced the recommendations made by our office, GAO, and NAPA and is taking action to improve Agency IT security and its management of export control and foreign national access. We will continue to provide aggressive oversight as NASA implements its Foreign National Access Management Program and works to improve its export control and IT security practices.

⁵ NASA OIG, "Review of ITAR and Foreign National Access at Ames Research Center" (February 26, 2014).



Gail A. Robinson
NASA Deputy Inspector General
Biography

Ms. Robinson is the Deputy Inspector General for the National Aeronautics and Space Administration (NASA). As the Deputy Inspector General, Ms. Robinson assists the Inspector General in managing the full range of programs and activities in the NASA Office of Inspector General (OIG).

Prior to her appointment as Deputy Inspector General, Ms. Robinson served as General Counsel for the U.S. Department of Justice OIG. In that position, she was responsible for providing advice to the Inspector General and OIG senior managers on a wide variety of legal matters.

Prior to joining the OIG community, Ms. Robinson worked at a private law firm and as an attorney for a non-profit organization. She also served as a law clerk on the United State Court of Appeals for the District of Columbia.

Ms. Robinson holds a B.A. in Political Science and English from Rutgers University and a Juris Doctor from the University of Pennsylvania Law School. She is married to Steven Larsen. She and Steven have two children.

Chairman PALAZZO. Thank you, Ms. Robinson.
I now recognize our final witness, Mr. Webster.

**TESTIMONY OF MR. DOUGLAS WEBSTER, FELLOW,
NATIONAL ACADEMY OF PUBLIC
ADMINISTRATION AND PRINCIPAL,
CAMBIO CONSULTING GROUP**

Mr. WEBSTER. Good morning, Mr. Chairman and members of the Committee. I thank you for the opportunity to present the National Academy of Public Administration's assessment of NASA's Foreign National Access Management.

NASA's charter to work cooperatively and share information with other nations while safeguarding its classified and proprietary information and assets can prove to be a challenging task. Security incidents involving foreign nationals at NASA research centers have led to justifiable scrutiny by NASA, the media, and Congress. Having a well-run Foreign National Access Management, or FNAME, program is in the best interest of NASA both in terms of protecting vital U.S. security and proprietary information, as well as capitalizing on the talents of foreign nationals.

The panel report describes a number of important steps the agency can take to improve Foreign National Access Management and has proposed 27 specific recommendations which I will summarize under six topic areas, the first of which is a recommendation to manage Foreign National Access Management as a program.

There is no systematic approach to FNAME at NASA. It is not managed as a program but rather in a more stove-piped organizational fashion. Individual headquarters elements produce program requirements which are in turn subject to broadly varying interpretations by NASA centers. Additionally, headquarters has inadequate means for determining the overall efficacy of these processes with a resulting broad range of outcomes, many of which are unsatisfactory.

The second topic area is to reduce the flexibility given to centers to interpret FNAME requirements. The panel believes that NASA FNAME directives are overly broad and subject to too much interpretation in the field combining too much flexibility for interpreting largely procedural processes with a stove-piped organizational structure that produces organizationally specific directives, results in inconsistent, ineffective, and often fundamentally flawed outcomes.

The third topic area is for NASA to determine critical assets and build mechanisms to protect them. NASA needs to improve how it protects all of its valuable technical—excuse me, technical data and proprietary information, not simply the proprietary sensitive and/or classified information potentially exposed to foreign nationals. The panel recommended that NASA strengthen its risk management capability by building on existing agency risk review processes to compile a comprehensive assessment of risks and threats.

The fourth topic area concerns information technology. The panel believes that NASA needs to correct long-standing information technology security issues. During this review, NASA IT professionals expressed strong concerns about the security of the agency's non-classified systems with some believing that these systems have

already been compromised. This finding is reinforced by other reviews of NASA's information technology, including those done by the NASA IG.

The fifth topic area concerns NASA organizational culture, which in many ways is exemplary, but when considering FNAME, NASA needs to change several aspects of its culture. The first aspect of NASA culture involves unnecessary competition between NASA field centers. Some centers struggle to solve problems that other centers have already resolved, wasting time and money. NASA also needs to approach its current budget situation in an organizationally united fashion.

A second aspect concerns accountability. The belief that individuals are not held accountable for ignoring or deliberately failing to comply with FNAME requirements is widespread at NASA and includes both managers and rank-and-file employees.

A third aspect of NASA culture that needs to be addressed is the organizational tendency to revert back to prior lax habits once a problem has been solved and the tension of the moment has passed.

The sixth and final topic area involves communicating the importance of these FNAME changes clearly, firmly, and consistently. The importance of security, the existence of real-world threats to NASA assets, and the need for improvements in handling foreign national issues have not been clearly and consistently communicated throughout NASA. Senior leaders must communicate their total commitment to an effective Foreign National Access Management program.

In closing, Mr. Chairman, let me note that I believe the Academy has provided NASA with a good template for building a more robust and effective FNAME program and that the agency has the right leadership and commitment to make that happen. The Academy is in a prime position to assist NASA and this Committee in implementing the panel's recommendations and providing the Committee with information to the extent to which NASA has complied with the recommendations. With the Committee's support and oversight, I am certain this program will continue to provide NASA with the foreign talent it needs to fulfill its mission while capably safeguarding sensitive information.

Thank you for providing me this opportunity to share these findings with you.

[The prepared statement of Mr. Webster follows:]



NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

1600 K Street, N.W., Suite 400
Washington, D.C. 20006

TEL: (202) 347-3190 FAX: (202) 223-0823
INTERNET: www.napawash.org

**WRITTEN STATEMENT
OF
THE HONORABLE DOUGLAS WEBSTER
PANEL MEMBER
NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

BEFORE THE
HOUSE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
SUBCOMMITTEE ON SPACE AND SUBCOMMITTEE ON OVERSIGHT**

JUNE 20, 2014

Good morning Mr. Chairman and members of the Committee. Thank you for providing me with the opportunity to present the National Academy of Public Administration's assessment of NASA's Foreign National Access Management practices. As a Congressionally-chartered non-partisan and non-profit organization with nearly 800 distinguished Fellows, the Academy brings seasoned experts together to help public organizations address their most critical challenges. The Academy is proud to have been chosen by NASA to review how it meets those challenges. Not only has the Academy conducted a number of important studies for NASA in the recent past, but both organizations share a common lineage in the person of James Webb, the second NASA Administrator and founder of the Academy in 1967.

NASA's charter directs the agency to work cooperatively and share information with other nations while simultaneously safeguarding its classified and proprietary information and assets. This can prove to be a challenging task. On the one hand, the threat of cyber-attacks and espionage aimed at government agencies by hostile nation-states and foreign adversaries is growing. On the other hand, collaboration and cooperation between nations are hallmarks of modern scientific endeavors.

Over the last year, security incidents involving foreign nationals at NASA research centers have led to justifiable scrutiny by the NASA Administrator, the media and the Congress. Recognizing these security challenges, NASA contracted with the Academy to conduct a review of its foreign national operations. How well NASA is able to balance their sometimes conflicting research demands, and what it might do to improve its processes for working with foreign nationals, were at the heart of this review.

NASA is one of the most accomplished agencies in the U.S. federal government and one of the most respected government entities in the world. To accomplish its mission, NASA works collaboratively with many nations on a broad range of scientific and engineering projects. Foreign national participation in NASA programs and projects is an inherent and essential element in NASA operations. No better illustration of this partnership is the fact that during 2013, NASA's international operations were being supported by over 600 cooperative agreements with 120 nations.

Having a well-run Foreign National Access Management program is in the best interests of NASA, both in terms of protecting vital U.S. security and proprietary information, as well as capitalizing on the talents of foreign nationals. This Academy review examined the Agency's entire Foreign National Access Management process from the initial request from a requestor or sponsor through foreign national vetting, credentialing, information technology security, counterintelligence, hosting and escort procedures, and export controls.

Before I present the Panel's findings I would like to note that NASA provided complete cooperation for this review and that NASA interviewees were candid, cooperative, and eager to

both offer suggestions and be involved in problem solving. Most NASA employees understood the challenge to share with, as well as to protect information from foreign nationals. During this review, Academy staff interviewed over 150 individuals during visits to 5 NASA Centers, NASA Headquarters and several other Federal agencies. They also reviewed all relevant Foreign National Access Management (FNAM) directives, reports, and studies.

The Panel is sensitive to current Federal budget challenges and has worked to keep its recommendations within achievable budget limits although some may prove to be resource-intensive. The Panel believes that NASA can not only make mission and security improvements to existing foreign national access systems by following its recommendations but can also realize long-term potential savings by managing its foreign national efforts in a more efficient and effective manner. This testimony will represent the major findings of the Academy Panel's review that generally follow the overarching areas NASA asked the Academy to review.

Organizational and Functional Relationships

There is no systematic approach to FNAM at NASA; rather, there are individual headquarters (HQ) program requirements coupled with individual Center approaches. Simply put, there is no overall FNAM program, just separate FNAM processes – credentialing, export control, counterintelligence, IT access, etc. – that are viewed as a series of related tasks performed by independent organizations and individuals, and which often result in less than optimal outcomes.

When FNAM is viewed through these individual lenses, the judgments made about its efficacy are often subjective and incomplete. Evaluations focus on the various components without consideration given to the overall effect of these processes. When coupled with the lack of good program audit mechanisms, the chances for things going wrong rise significantly. This is particularly ironic, given that NASA is one of the most successful organizations in the world at practicing high-quality program management. The Panel has no doubt that any effort by the Agency to take a Program Management approach to FNAM would be successful.

FNAM Directives

An integral part of this review involved assessing the efficiency and effectiveness of the guidance provided by specific NASA publications pertaining to FNAM. In general, the Academy found that NASA Procedural Requirements (NPRs) and NASA Policy Directives (NPDs) were comprehensive, well-written, and easily accessible through NASA's online library. These documents provided answers to the "who, what, why, where, and when" questions, but did not adequately provide effective and practical guidance on "how" responsible individuals, officials, and entities were to perform their designated tasks. This was determined to be particularly true with processes that involved multiple individuals and organizations.

Through the interviews conducted at the Centers, it was clear that employees and contractors were aware of the existence of the FNAM publications, but those documents were infrequently utilized in the performance of day-to-day tasks and assignments. Most personnel relied on their own experience or that of their peers when faced with an issue or problem. In some cases, Centers have developed and published their own procedural requirements that were found to be more practical and user-friendly.

The Panel notes that uniformity and consistency in organizational performance by other federal agencies is directly correlated with the existence and routine use of agency-wide, clear, and concise direction and guidance. Most often, this guidance is disseminated through the publication of manuals and guidelines that provide simplified and practical instruction on the performance of specific tasks, as required by procedural and policy mandates. This observation was independently validated by NASA interviewees who noted the need for specific guidance on how to best perform certain FNAM functional requirements – that is – vetting, credentialing, sponsoring, escorting, and export control.

NASA states that compliance with each NPR and NPD is mandatory, and accountability for the aspects of each program and function is established. Despite these statements, the Academy found that there is little accountability for non-compliance when identified through specific incidents or periodic assessments. This validates the identified perception among NASA personnel that “mandatory compliance” means little, as there are few, if any, consequences for deliberate or inadvertent violations of the mandates. This combination of overly-broad directives combined with limited accountability has lead to both varying processes and undesired outcomes.

NASA Decentralized Management

NASA needs to take steps to reduce the decentralized authority given to Centers for implementing FNAM and other largely procedural or enterprise-wide processes. NASA has a longstanding, highly decentralized organizational structure, with very independent field Centers. Allowing Centers great latitude to implement policies to fit their particular circumstances has the advantage of improving prospects for buy-in and creating policies and procedures which best fit local circumstances, but it can hamper enterprise solutions when such solutions are required. Different interpretations of NASA Procedural Requirements by individual Centers can result in widely varying FNAM performance among Centers.

If too much flexibility in largely procedural processes (which is what much of FNAM consists of) is coupled with a “stovepiped” organizational structure as mentioned above, then results become less predictable and often the opposite of what was intended. The benefits of tailorability and flexibility are outweighed by the inconsistency and often poor outcomes that result from this

approach. Moreover, “reinventing the wheel” at Centers precludes sharing of best practices and lessons learned that contribute to increased effectiveness and efficiency.

Tracking Foreign Nationals at NASA

Individuals requiring access to NASA facilities undergo vetting via an automated system designed to capture and store identity and credential data based on the visit type, residency and country affiliation. A requestor must submit a request for a visit via the **Identity Management and Account Exchange (IdMAX)** system which is an automated workflow tool used to process individuals for access to NASA facilities. IdMAX provides a record for identity confirmation and type of access (visitor, staff, contractor, foreign national), whether IT access is allowed and to what level. It is a single repository for anyone with access to NASA facilities or NASA data. The database asks a series of questions to determine level of access based on confidence and risk factors and is part of a larger program called Identity Credential and Access Management (ICAM).

The review found inconsistent application of and compliance with established policies, as well as broad interpretation of the NPRs regarding IdMAX. Centers have established different processes for the same activities, e.g. processing foreign nationals onto the facility and deciding who is allowed access to the systems.

Information Technology Security

A 2013 NASA IG Audit on Information Technology Governance stated that the NASA CIO has a restricted ability to standardize assets across the Agency to ensure that security policies are adhered to. The Office of the CIO also has very limited capabilities for monitoring the Agency’s mission networks and has to instead rely on self-reporting of vulnerabilities by the mission IT staffs. These limitations are further compounded by the fact that NASA does not have a complete inventory of IT assets. The Academy’s research and findings in these respects are consistent with the IG report.

NASA systems are decentralized and the responsibility for management and security is delegated to the Centers. Center CIOs and system owners have considerable autonomy in managing their systems. System owners determine access controls and have the ability to add networks or connect to external networks. Most Center CIOs have the ability to monitor the “health” of their networks locally, but no authority to require that system owners allow monitoring by the Center or the Security Operations Center (SOC). Most of them noted that they have no ability to prevent mission managers from establishing stand-alone systems or adding back end connections to the network.

NASA has a culture of information sharing and Agency information systems were designed to facilitate such sharing as opposed to identifying, monitoring or preventing potential threats. A 2010 NASA memorandum highlighted the state of NASA systems, and the impacts of unauthorized access to Agency systems, to include *“loss of productivity, theft of intellectual property (data exfiltration), and public embarrassment.”* A NASA white paper from that same year outlined the state of NASA’s compromised environment, providing details of the threats the Agency faced, the vulnerabilities that were being exploited and detailed examples of recent incidents.

Due to the fact that the NASA systems lack the necessary controls to protect information, allow foreign nationals access to the networks, and allow remote access, the Panel concludes that the NASA networks are compromised. Publicly available reports on systemic data breaches across the country, NASA’s own internal reports, and briefings given to Academy staff leave little doubt that information contained on the NASA IT systems is compromised.

Counterintelligence Awareness and Education Programs

NASA directives state that the purpose of the counterintelligence and counterterrorism (CI/CT) program *“is to detect, deter, and neutralize potential threats posed by foreign intelligence services (FIS), other foreign entities, and acts of terrorism to include trusted insiders who would engage in activities on behalf of an FIS or terrorist entity.”* When NASA’s CI Program was created, no additional personnel were hired. Instead, CI responsibilities were given to Center security personnel as ancillary duties. A 2000 study of NASA’s counterintelligence capabilities recommended that the CI personnel be assigned to CI matters on a full-time basis, and be responsible to both Center management and HQ. NASA assigned CI Special Agents (CISAs) to work only CI/CT matters and then centralized the CI/CT program under the Director of the CI/CT Division at HQ.

The Panel found that the current number of personnel assigned to the CI/CT Program is inadequate to formulate, manage, and perform effective CI Awareness and Education programs and that Center-based CISAs would function more effectively if placed under Center management with close HQ oversight. The Panel also found that CI awareness briefings do not seem to be a priority and that CI awareness and education at the Centers and at HQ varies greatly, with some being ineffective.

The CI travel briefing program appears to have the most consistency and clarity of the CI programs, but it reaches only a limited number of personnel. The Academy found that most CISAs appear to be very conscientious in contacting travelers to Designated Countries and high-threat areas, and in providing updated travel briefings. Some Centers send significantly more foreign travelers to Designated and high-threat countries than others, and the Special Agents in

these high-travel Centers are especially diligent in their attempts to brief all of their frequent travelers.

Procedures for Hosting and Escorting Foreign Nationals

Hosting of visitors to NASA facilities, including foreign nationals, can encompass all phases of FNAM – from initial identification of foreign visitors through termination of their physical or remote access to NASA assets. This can also involve policies, procedures, and processes pertaining to foreign national vetting, badging, escorting, accessing facilities and information technology systems, export control issues, monitoring, awareness and training, as well as the interrelationships of the NASA HQ and Center organizations.

NASA Headquarters Officials and Center Directors have not adequately communicated that strict compliance was and is required for foreign national hosting, sponsoring, and escort policy and procedures. There is little uniformity and consistency in the application of the procedural requirements for hosts/sponsors and escorts among the Centers. This includes briefings and debriefings, the documents used to delineate the physical and/or logical access plans, and the duties and responsibilities of those involved in the process.

FNAM procedures, particularly for those individuals from Designated Countries and high-threat locations, are considered by requesters, sponsors, and escorts to be too complex, confusing, and time-consuming. This has created a reluctance or refusal to utilize the expertise and skills of foreign nationals by some NASA sponsors. Integrated Functional Reviews and CI/CT Evaluations which NASA conducts do not specifically address the performance of the tasks pertaining to hosting/sponsoring and escorting foreign nationals, and the required briefings of sponsors and escorts of foreign nationals have not adequately conveyed the risk that an individual might pose to NASA assets.

Export Control

NASA's export policy directive clearly states that it *"is NASA policy to ensure that exports and transfers of commodities, technical data, or software to foreign persons are carried out in accordance with the United States export control laws and regulations, and Administration and NASA policy."* The Export Control program needs a more standardized and systematic approach in furtherance of its export compliance objectives, as well as better audit and review mechanisms. NASA senior leaders also need to more strongly endorse the critical importance of such controls. The training provided to Center staff members who need to be aware of export control issues is Center-centric and widely-varied. Some Centers have mandated training for all staff on an annual basis. Others take a more *laissez-faire* approach with training either being optional or, if mandatory, provides no sanctions against those who fail to take the training.

These *laissez-faire* approaches tend to create misunderstandings and even a degree of mistrust and hostility between the various parties. Academy staff heard numerous complaints from researchers about Center Export Administrators (CEAs) and their “unnecessarily bureaucratic” and “time-consuming” reviews and conversely, heard complaints from CEAs about “unreasonable” demands for turning-around documents which always seem to be submitted for review at the last minute. Such complaints indicate a lack of communication about both time frames and rationales for these types of security measures. In summary, the Panel Export control training requirements are inconsistent, the training is confusing and inadequate, and the rationale for such training is often poorly understood.

Monitoring FNAM Compliance and Performance

NASA needs more robust mechanisms for ensuring that FNAM policy requirements are being met by field Centers. There have been recent improvements by NASA HQ in auditing and assessing field Center FNAM efforts but more needs to be done. Absent an improved system of oversight, the Agency will remain uncertain about how well FNAM is being conducted. There are a number of time-tested approaches to this but one which needs to be considered is the use of cross-functional teams to review Center FNAM operations. Such teams could review the individual program compliance metrics (e.g., export control, credentialing, etc.) as well as the overall performance and outcomes of FNAM at the Center. Team membership should include not only HQ program specialists but also FNAM staff from other Centers to both provide a field perspective and to propagate the cross-fertilization of ideas.

As opposed to doing the organizational-specific compliance audits as is the practice today, the teams’ reviews should result in comprehensive Center-specific assessments in which all physical, technological and informational assets are identified; actual and potential threats to those assets evaluated; risks assessed; protective strategies developed; and resource requirements prioritized. These assessments should be incorporated into the OMB Circular A-123 Internal Controls reporting process at the Center and HQ organizational levels.

Asset Protection

The task of protecting NASA’s assets – its facilities, personnel, technologies, and information – is a multi-dimensional responsibility involving every NASA civil servant, contractor, and organization, as well as the support and assistance of other agencies. The successful performance of this task is dependent on completion of a number of interrelated functions – identification of assets requiring protection, accurate intelligence regarding threats, design and implementation of protective strategies, education and awareness of NASA personnel, and continuous evaluation to ensure threats are countered commensurate with their importance. This requires a comprehensive approach to risk management, employing the best practices available.

During this study, the Academy observed the following regarding NASA's asset protection efforts:

- Centers differ in their efforts to identify assets that require protection, with responsibility placed on several different components.
- Threats have not been adequately conveyed to Center personnel.
- Extensive instructional/training material available through the FBI, Department of Energy (DOE), Office of the National Counterintelligence Executive (NCIX), and other Intelligence Community (IC) agencies has not been utilized to educate NASA staff on the threats posed by insiders, hostile intelligence services, terrorism, and economic espionage.
- Specific intelligence regarding threats posed by foreign nationals and insiders to specific NASA assets is available from intelligence community (IC) agencies, but has been inconsistently utilized to educate NASA personnel.
- Detailed policies, procedures, and instructions regarding comprehensive approaches to asset protection have been implemented by other agencies, particularly DOE, and should be reviewed for possible utilization by NASA.
- Independent and Management Assessment and Evaluations, employed by IC agencies, should be regularly utilized to determine the effectiveness of NASA's asset protection efforts, gaps in those procedures, and assurance that proper resources are committed commensurate with the risk.

NASA needs to reconsider how it assesses and protects its information and security assets in the field. While this review has focused on FNAME, the Panel believes that a broader approach to asset protection and oversight is needed. NASA facilities, personnel, technologies, and information are highly regarded and of great interest to the world. That interest extends to some countries, governments, organizations, and individuals whose intent is to compromise those facilities, co-opt the personnel, and steal those technologies and information. While NASA currently conducts annual threat assessments at every Center by the Protective Services office, counterintelligence special agents, and the CIO, those assessments address only the areas of responsibility of those individual offices. They are not comprehensive, Center-specific assessments that consider all the elements necessary to fully protect NASA's assets.

The Panel believes NASA needs an Asset Protection Oversight Board to oversee the safety and security of NASA assets in the field. The overall goal of the Board is to protect all of NASA's valuable technical data and proprietary information, not simply the data potentially exposed to foreign nationals and to also compile threat assessments from the various elements into comprehensive Center and agency threat/risk assessments. These assessments could be incorporated into NASA's risk management and internal control process. By establishing a

mechanism for comprehensive, Center-specific assessments, NASA could identify and prioritize vulnerable assets, assess protective strategies, allocate resources commensurate with the risk, and evaluate the overall asset protection efforts.

NASA Internal Controls and Risk Management

NASA needs to reconsider how it assesses and protects its information and security assets in the field. The NASA Management System Working Group (MSWG) serves “as the Community of Practice (COP) for NASA internal controls activities and the effective integration of internal controls into any agency-wide Integrated Management System (IMS).” The MSWG scope covers NASA Headquarters, NASA Centers, and their associated facilities. This charter is consistent with the broad scope intended by OMB Circular A-123. Unlike many federal agencies that implement internal controls with an overly strong focus on financial reporting, MSWG is a newly-revised organization under the direction of a new Associate Administrator.

While responsibility for internal controls over financial reporting is placed under the NASA Chief Financial Officer, overall responsibility for NASA-wide internal controls – and providing direction to the MSWG – is placed under the Director, Office of Internal Controls and Management Systems, who in turn reports to the Associate Administrator for Mission Support. This management structure clearly signals NASA’s recognition that internal controls apply universally across all areas of the agency, and is not focused exclusively on financial reporting.

While NASA’s intent is to establish an internal controls management framework across all organizational elements, the effective implementation of the policy outlined is not consistent. A Senior Assessment Team (SAT) oversees the internal controls program and has as members representatives from all program and functional areas of NASA. However, the SAT is able to assess, prioritize and correct control deficiencies only to the degree such deficiencies are brought to the SAT’s attention. Unfortunately, there are management processes operating at the Center level that identify problems and risks, but that are disconnected from the internal controls process.

NASA’s Surveys, Audits and Reviews (SAR) Policy generates insights at the Center-level on various risks and problems. However, the only formal connection between this set of processes and the internal controls program is that Center Directors submit their Certification Statements to HQ to be included in the Agency’s annual Assurance Statement. To the degree that the SAR program identifies risks associated with internal operations and processes, there should be a communications path to ensure such risks and control deficiencies inform the internal controls program. Moreover, all control deficiencies identified at the Center level are not currently required to be reported to Headquarters. As a result, there is no ability of the SAT to independently assess the degree of completeness of information forwarded to the SAT by the

Center. Meaningful transparency would allow the SAT complete access to internal controls findings at the Center level.

The Panel notes that NASA's annual Statement of Assurance (SoA) rolls up/includes risks that are obtained from the Centers, and NASA policies make it clear that internal controls are the responsibility of the Center Directors and other appropriate officials who also are required to perform self-assessments and submit Certification Statements. However, the Panel believes that the current process is not sufficient and that an oversight entity is needed by NASA to focus on the following goals and objectives:

- Develop a multi-disciplinary template for use by Center personnel to periodically identify assets to be protected, internal and external threats based on self-assessments and intelligence received, resource and/or technological enhancements needed, and deficiencies identified and/or improvements required.
- Collate the comprehensive Center risk assessments into an agency-wide risk assessment to be provided to executive management for determining resource allocation, budgetary requests, and organizational performance assessments.
- Center and agency risk assessments should be provided to those entities having internal control responsibilities, to include the CFO and MSWG.
- Enhance liaison with Intelligence Community (IC) agencies to disseminate and vet Center and agency risk assessments, obtain current intelligence on targeting of NASA assets by individuals, organizations, or governments, leverage successful protective strategies developed by those agencies, and utilize their training and awareness materials and resources to educate NASA civil servants and contractors.
- Establish an Independent Assessment/Inspection team to periodically assess and evaluate each Center's organizational and functional performance in all facets of asset protection, to include FNAME, physical security, IT security, export control, training and awareness, and liaison. Particular emphasis should be placed on evaluating organizational interactions and relationships, with input from Center management and affected personnel.

The Panel believes that establishing a mechanism for comprehensive, Center-specific assessments and creating an oversight entity to manage this process would allow NASA to fully integrate both its HQ and Center internal controls and risk management efforts into a comprehensive and cohesive effort.

Potential Organizational Changes

There are a several organizational changes NASA can make to strengthen FNAME. The Panel believes that Counterintelligence Staff in the field would function more successfully if they were integrated into the field Protective Services staff under the ultimate supervision of the Center Director. Although plausible arguments can be made to keep the CI staff under HQ management, observations by Academy staff during field Center visits, as well as the CI/CT assessment of 2000, led to the conclusion that the special agents would be more integrated into overall operations, and consequently more successful, if put under Center management. The danger of having them diverted to non-CI tasks as has taken place in the past when they were under Center management, can be mitigated by having clear policies forbidding same and strong audit reviews to make sure it is not happening.

The Panel also thinks the time is appropriate for an elevation of the organization with the primary responsibility for Foreign National Access Management – Protective Services in NASA Headquarters – to be moved onto a level with more direct reporting responsibilities to the Office of the Administrator to ensure that these critical issues receive the appropriate amount of leadership attention. The Panel believes that more visibility for HQ OPS coupled with a stronger relationship with field counterparts will help to strengthen NASA's overall security.

Because of the strong link between a successful FNAME program and effective risk management and internal controls, it is also suggested that NASA consider moving the Office of the Internal Controls and Management Systems (OICMS) from the Mission Support Directorate to a staff function under the Administrator. The OICMS is not simply a support function, but a policy and monitoring function that must provide oversight to ensure an effective internal controls program across all of NASA. The proposed realignment would better reflect the organizational policy and oversight responsibilities that should be exercised by OICMS.

Finally, certain key FNAME-related jobs in the field, specifically the Chiefs of the Office of Protective Services, Center Export Administrators, and Counterintelligence Special Agents should have formal, recognized relationships with their HQ counterparts. Forging a strong linkage (a "dotted-line" organizational relationship) between the HQ and field entities can only strengthen FNAME. Currently, Center OPS Chief selections and evaluations require the endorsement of the HQ Assistant Administrator for OPS. Although there are consultations regarding selections, Academy staff could not find evidence that HQ endorses Center OPS Chiefs' evaluations.

The NASA CIO is currently the supervisor of Center CIOs but there are two observations the Panel makes about this: first, some Center CIOs interviewed by Academy staff were unaware of this reporting responsibility; and, second, the Panel believes mission CIOs should also require the NASA CIO's endorsement prior to their selection and annual evaluation. That currently is

not the practice at NASA. The Panel believes that forging a strong link between these line and staff positions while still maintaining a strong field-based approach will help ensure that asset protection is well done and remains a priority.

Competition between Field Centers

Unnecessary competition between Centers is counterproductive. Competition can potentially hamper non-mission activities that often require a more structured, consistent approach, and most particularly, the sharing of best practices. Having Centers struggle to solve problems that other Centers already resolved, which the Academy staff observed during their Center visits, is a waste of time and money and jeopardizes the success of the program. When it comes to FNAM, Center competition does not “improve the breed.” It actually hurts in two ways: Centers with solutions might be disinclined to assist “competitors” and Centers experiencing problems might be concerned about exposing weaknesses in their operations.

An additional consideration is the need for NASA to approach its current budget situation in an organizationally united fashion. Competition between Centers is anathema to this requirement. NASA budget constraints – “flat is the new up” – require a mission approach that drives Centers to work collaboratively with each other and HQ, to ensure that scarce mission-critical resources are not squandered by unnecessary redundancy and waste.

NASA Culture

Any discussion of Foreign National Access Management problems and potential solutions must take into account NASA culture which plays an important role in every aspect of NASA operations. NASA is seen as a desirable place to work with a highly-educated, talented and committed, but rapidly-aging, workforce. In 2013, it was ranked “Best Place to Work in Government” in an annual poll. The Agency has an important, high-profile mission and the NASA “brand” is recognized and admired throughout the world. NASA culture plays an important role in creating these attitudes and perceptions.

NASA research is done largely in a collegial atmosphere with the grounds on each Center being referred to as a “campus.” This fosters the sharing of information, an essential element in research, but can create tension between the need to collaborate and the need to protect classified or otherwise sensitive information. There is also a tendency for some staff to find a “work-around” for procedures and policies they do not agree with or believe to be erroneous, including some FNAM requirements. NASA also often uses an informal (i.e., non-hierarchical) approach to management of people and processes. Directives, and orders, can be seen more as “guidance” as opposed to mandatory policy and procedural requirements that must be adhered to. This can lead to communications breakdowns and negative outcomes.

NASA leaders shared the concern with Academy staff that after fixing a problem, the Agency has a tendency to lapse back into old habits once the spotlight is off the area under review, in this case, FNAM. A number of NASA leaders also noted that the Agency tends not to hold individuals accountable even when they make serious, preventable errors. Whenever an example of such an error was mentioned during the interviews, Academy staff would follow-up with: *what happened to those responsible for the error?* In almost every instance, the answer was either “nothing” or “I don’t know.” The belief that individuals are not held accountable for ignoring or deliberately failing to comply with FNAM requirements is widespread and includes both managers and rank-and-file employees.

If there are no consequences for ignoring or significantly deviating from a policy requirement or directive, then the chance of the policy or directive being implemented as intended decline dramatically. An important element in changing this attitude and driving compliance is the certainty that processes and outcomes will be reviewed by external entities. This is not to suggest a harsh or unforgiving approach to discipline; the goal is not punishment but reinforcement of behavioral norms.

Panel Recommendations

The Panel made 27 recommendations to NASA as to how it can improve its Foreign National Access Management in its final report which can be summarized into the following six headings:

1. **Manage FNAM as a Program.** The Panel proposed a number of steps for NASA to take which would begin to coordinate efforts and secure better results including realignment of both field and Headquarters organizational elements, strengthening the oversight capabilities of headquarters, and, improving training by developing comprehensive, integrated curriculums and lesson plans.
2. **Reduce the flexibility given to Centers to interpret FNAM requirements.** The Panel recommended that NASA Headquarters write a comprehensive and detailed FNAM operating manual covering all functional aspects of the program. Currently, FNAM directives can be found in several different publications, each with their own Headquarters and field constituencies. Headquarters staff should work in consultation with knowledgeable field staff to create this manual.
3. **Determine critical assets and build mechanisms to protect them.** The Panel envisions the creation of an Asset Protection Oversight Board which would use the results of the Independent Review Team’s assessments of individual program compliance metrics as well as overall performance and outcomes of FNAM and the adequacy of the comprehensive threat/risk assessment at each Center.
4. **Correct longstanding information technology security issues.** The Panel believes NASA needs to identify and protect sensitive, proprietary information in a manner that does not prevent system owners from meeting their mission needs. Among the specific

recommendations in this area are for NASA to establish clear, specific, and mandatory requirements for all Centers to follow regarding remote access of their information technology systems and that the NASA Chief Information Officer be given more control over IT operations in field Centers.

5. **Work to change several aspects of NASA culture.** Included in this are the recommendations to reduce unnecessary competition between field centers, ensure that accountability for conforming to FNAME requirements is established, and finally, to guard against the organizational tendency to revert back to prior lax habits once a problem area has been addressed.
6. **Communicate the importance of these FNAME changes clearly, firmly and consistently.** The importance of security, the existence of “real world” threats to NASA assets, and the need for improvements in handling foreign national issues have not been clearly and consistently communicated throughout NASA. Senior leaders must firmly establish and communicate their total commitment to an effective Foreign National Access Management program that enhances cooperation while safeguarding information.

In closing, let me note that the Academy was pleased and honored to work with NASA and the Committee on this review and to present this testimony today. I believe that we have provided NASA with a good template for building a robust and effective Foreign National Access Management program and that the Agency has the right leadership and commitment to make that happen. The Academy is in a prime position to assist NASA and this Committee in implementing the Panel’s recommendations and providing the Committee with information to the extent to which NASA has complied with the recommendations.

With the Committee’s support and oversight, I am certain this program will provide NASA with the foreign talent it needs to fulfill its mission while capably safeguarding sensitive information. Thank you for providing me this opportunity to share these views with you.



NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

1600 K Street, N.W., Suite 400
Washington, D.C. 20006

TEL: (202) 347-3190 FAX: (202) 223-0823
INTERNET: www.napawash.org

The Honorable Douglas Webster Narrative Bio

Dr. Doug Webster served a 21 year career as a US Air Force officer, after which he entered management consulting providing advisory services to federal agencies. In 2004 he temporarily reentered the federal government to serve with the Coalition Provisional Authority in Baghdad, Iraq, as the Principal Finance Advisor to the Iraqi Ministry of Transportation. In this capacity, he functioned as the de facto CFO for a ministry of nearly 40,000 persons. In 2007, Dr. Webster was appointed by the President and confirmed by the Senate to serve as the Chief Financial Officer of the US Department of Labor. In this capacity, he provided financial leadership to a department with a budget exceeding \$54 billion. After leaving the Department of Labor at the end of the prior administration, he served as the Deputy Director of the Department of Defense Business Transformation Agency. He currently serves as the founder and president of the Cambio Consulting Group, an organization focused on helping federal agencies improve stakeholder value through strategic planning, cost management, performance management, enterprise risk management, and organizational change management.

Dr. Webster also led the founding of the Association for Federal Enterprise Risk Management, and the establishment of the annual Federal Enterprise Risk Management Summits beginning in 2008. He serves on the Board of Directors of Pentagon Federal Credit Union, an \$18B financial services organization with over 1.2 million members, chairs the board risk committee, and serves on the real estate, strategic planning, and mergers and acquisitions committees. He also serves on the board of the PenFed Foundation, a 501(c)3 charity focused on helping veterans and their families. He has a BS in Engineering, a MS in Systems Management, and a Doctorate in Business Administration. He is a co-author of the books *Activity Based Costing and Performance* (AMS, 1994), *Chasing Change: Building Organizational Capacity in a Turbulent Environment* (Wiley and Sons, 2009), and *Managing Risk and Performance: A Guide for Government Decision Makers* (Wiley and Sons, 2014).

Chairman PALAZZO. Thank you, Mr. Webster. I thank the witnesses for their testimony.

Reminding Members that Committee rules limit questioning to five minutes, the Chair will at this point open the round of questions. The Chair recognizes himself for five minutes.

The NASA IG report on Bo Jiang stated Jiang admitted that the laptop computer he carried with him when he attempted to leave the United States in March contains some NASA information. According to these Department of Justice officials, the nature of the information on Jiang's computer and how he obtained it remains under investigation. The OIG report also states that Jiang had access to a NASA employee's computer that specialized in technology that would allow for real-time video image enhancement to improve aircraft safety by making it easier for pilots to fly in poor visibility conditions.

Ms. Robinson, are you aware of the status of this investigation? Has anyone looked into whether Jiang transferred any information electronically prior to being stopped at the airport since he had access to NASA information long before he attempted to leave the country?

Ms. ROBINSON. Mr. Chairman, to my knowledge the investigation is still open. The FBI is the cognizant law enforcement agency in that regard.

Chairman PALAZZO. So it is ongoing and active?

Ms. ROBINSON. As far as I am aware, it is still open.

Chairman PALAZZO. Okay. The IG's report on Bo Jiang incident states that from an individual perspective, the preponderance of the evidence available to us suggest that one of Jiang's sponsors inappropriately authorized Jiang to take the laptop to China. Mr. Keegan, has that individual been reprimanded, and if so, how?

Mr. KEEGAN. We appreciate the Office of Inspector General—

Chairman PALAZZO. Your mike, please.

Mr. KEEGAN. We appreciate the Office of Inspector General's report on the entire Bo Jiang incident and we have concurred with all those recommendations.

With respect to personnel actions, I can't discuss them here, but I can assure you that that report got the personal attention of the Administrator and appropriate actions have been taken or will be taken at the appropriate time.

Chairman PALAZZO. Will you be able to provide some of that information to professional staff, Committee staff?

Mr. KEEGAN. I don't think I can discuss specific individuals with respect to personnel actions. I would also note because of the ongoing investigation, there are some actions that NASA could not have appropriately taken until that investigation is concluded.

Chairman PALAZZO. Okay. Thank you.

The IG's Ames report states that a foreign national working at Ames inappropriately traveled overseas with a NASA-issued laptop containing ITAR-restricted information. The report also stated, "we believe several Ames managers exercised poor judgment in their dealings with foreign nationals." With respect to ITAR issues, we found that several foreign nationals, without the required license, worked on projects that were later determined to involve ITAR-restricted information. In addition, on two occasions, a senior Ames

manager inappropriately shared documents with unlicensed foreign nationals that contained ITAR markings or had been identified as containing ITAR-restricted information by NASA export control personnel.

Mr. Keegan, similar to the other question, were any of these individuals reprimanded, and if so, how?

Mr. KEEGAN. As noted in Ms. Robinson's opening statement, there was a great confusion and disagreement at Ames about what was the appropriate roles and responsibilities and whether export-controlled information was involved or not, and those pointed to weaknesses in our guidance and in our policy and procedures, and we have concurred with the recommendations to improve those items and we are moving to implement those changes.

Again, with respect to personnel actions, I can't discuss those but I will say in that case, again, the Administrator personally got involved with that report in response to it and appropriate actions have been taken.

Chairman PALAZZO. Okay. Thank you, Mr. Keegan. And we respect the fact that you are not going to be able to directly talk about personnel actions. That is private in nature. We may delve more into it at a later time but, you know, it goes back to the culture of, you know, just kind of shrugging off these incidents, not taking them seriously. And if senior officials don't reprimand, you know, the parties that are allowing this sensitive information to possibly be compromised, it sends the wrong message across the entire institution. So we hope you will continue taking these recommendations and not just concurring with them but actually implementing them and then punishing those going forward if they continue to violate ITAR restrictions.

My last question, the GAO report states that NASA headquarters export control officials and Center Export Administrators lack a comprehensive inventory of the types and location of export-controlled technologies and centers limiting their ability to identify internal and external risks to export control compliance. This is not new. The GAO report also recognized that NASA's lack of comprehensive inventory of its export-controlled technologies is a long-standing issue that the NASA Inspector General identified as early as 1999. I know Ms. Martin's testimony touched on this.

So Mr. Keegan, how can NASA protect what it doesn't know it has?

Mr. KEEGAN. I think the reports that you cited pointed out opportunities for NASA to improve its sort of centralized approach to categorizing the risk and the vulnerable technologies in our system. NASA has concurred with those recommendations and is consulting with our own internal Chief Technologist Office, Protective Services and the Mission Support Directorate to identify existing catalogs of technologies that would prove useful in implementing a risk-based assessment of Key technologies. We are also working to improve our internal reviews and audits in both export control and Foreign National Access Management and to strengthen compliance and accountability mechanisms to address the issue you raised in your comment that individuals need to be held accountable for knowing their responsibilities and for fulfilling those responsibilities.

Chairman PALAZZO. Well, I appreciate that. You know, the issue has been out there for 15 years. You know, Congress wants to trust NASA that they are going to take corrective action this time and fix the problem.

At this time I recognize the Ranking Member, Mr. Maffei.

Mr. MAFFEI. Thank you, Mr. Chairman.

It seems to me that we are just lucky that even more sensitive information hasn't been compromised. I will ask Mr. Keegan, why is international collaboration so critical to NASA's mission and should we just suspend international cooperation until these security concerns are addressed?

Mr. KEEGAN. Cooperation with international nations is actually part of the NASA's foundational legislation, the Space Act, and NASA has derived great benefits from our international cooperation. Over half the operational science missions have significant international participation and contributions. The International Space Station obviously depends heavily on international contributions, and humans have inhabited that facility continuously for 13 years. So a lot of NASA's best, greatest accomplishments have depended on international contributions and cooperation.

Given those benefits, we need to balance that with our duty to protect sensitive export-controlled information, and that is, you know, a balance that has been mentioned by a number of the reports we are talking about today. And when the Administrator first became aware of issues, that sort of shook his confidence that we were able to fulfill that responsibility. Therefore, he took immediate action to stand down, for example, to issue a moratorium on foreign national access until each center director could validate their compliance with existing rules and policies through internal reviews, and he also took down a NASA website, the NASA NTRS website, which is the website through which we share publicly the results of NASA's scientific and technical research until we could validate that all the documents, over a million on that website, had proper internal controls.

And as a result of these actions and other actions we are taking in response to the reports we are discussing here today, NASA is confident that we can assure the security of sensitive export-controlled information.

Mr. MAFFEI. All right. Thank you, Mr. Keegan.

Mr. Webster, are you satisfied that NASA is making due progress in addressing the concerns of your organization?

Mr. WEBSTER. Well, I can say that they were very receptive and very cooperative with the study. The study has not reviewed the progress that they have made since our recommendations, and so that progress remains to be seen.

Mr. MAFFEI. Ms. Martin and Ms. Robinson, can you comment on the progress since the study?

Ms. ROBINSON. We have not gone to see what NASA has done since the study in terms of an audit or anything like that, but I agree that they have been very receptive to our recommendations and I believe they are working hard on the matter.

Ms. MARTIN. Likewise, NASA agreed with all seven of our recommendations. We were certainly encouraged that the Administrator issued a memo to all staff reiterating the importance of ex-

port controls and also met with the Center Export Administrators. So that is an example of the tone from the top. But again, we have not fully evaluated all of the actions.

Mr. MAFFEI. Mr. Keegan, Mr. Webster talked about, in his testimony, some cultural changes that would need to take place at NASA. Those are very challenging for any Administrator to implement. Do you feel if the current Administrator is able to change some of the culture at NASA? How are you approaching that?

Mr. KEEGAN. In a couple ways. NASA is looking at our whole competition model as to the advantages and to the drawbacks of that model and we acknowledge that that sometimes creates incentives not to share information across centers in a way that is helpful to NASA as a whole. I think the Administrator has emphasized directly both to me and Associate Administrator Robert Lightfoot and to the Center Directors and Mission Directors who report to Mr. Lightfoot that they will be held accountable for implementing the actions in response to these reports and for emphasizing and complying with the requirements in these areas and for seeing that that is done in their organizations.

Mr. MAFFEI. I thank the witnesses and yield back.

Chairman PALAZZO. I now recognize Dr. Broun for five minutes.

Mr. BROUN. Thank you, Mr. Chairman.

Mr. Keegan, I am a little perplexed—actually a little more than perplexed about NASA's priorities toward protecting sensitive or secure information. Chairman Palazzo has called this hearing because of multiple points highlighting NASA's poor oversight and management in protecting sensitive information, yet your written statement discusses a request for "new" statutory authority for—to allow NASA to withhold from the public certain technical data requested under FOIA.

It is also my understanding that NASA has resisted the Committee's efforts to make public the NAPA report even with an offer for the agency to redact it.

Now, don't get me wrong; I am certainly not encouraging NASA to release sensitive information. But to be clear, it is NASA's position that the entire NAPA report, the entire NAPA report, is sensitive and that no aspect whatsoever can be released without compromising security vulnerabilities.

If so, would you please provide this Committee a detailed list of the specific passages and concerns NASA is worried about releasing? For instance, I find it hard to believe that the background section has anything of concern within it.

Mr. KEEGAN. NASA appreciates the comprehensive, thorough, and detailed analysis that the NAPA panel did on our security vulnerabilities and problems with our systems and processes, internal deliberations, IT assets, and so forth. We also appreciate the fact that they rank-ordered their 27 recommendations with an assessment of risk associated with each one so that we could prioritize our actions and response. But the combination of that information would serve to make vulnerable the very information that we are trying to protect by improving our processes in these areas. The information that would provide—you know, too much information about our vulnerabilities—is interwoven throughout the report, so to meaningfully and thoroughly redact it, to take that

out, would in our opinion make the report no more useful than the executive summary which summarizes the six areas of recommendations and at the same time still pose a risk to security. So NASA has no plans to publicly release that report, although we have provided a copy of the full report—an SBU full report to the Committee Chairman at his request.

Mr. BROUN. Mr. Webster, do you believe there is any specific information in the NAPA report that is sensitive, and if so, could it be redacted that the entire—that the public could read the rest of the report? We have just heard what Mr. Keegan said.

Mr. WEBSTER. I do believe that there is some information in there that is sensitive and I do understand the basic underlying premise that you can take individually—information that is standing on its own is not sensitive, but when you piece it together with other related pieces of information, it can provide insight to an adversary that might be useful they would otherwise not gain. So I understand the philosophy. I am not in a position to judge if you will because we haven't done that analysis and we don't really have that charter to provide that type of analysis, but I do understand the basic logic.

Mr. BROUN. Ms. Robinson, ironically, it appears that—as though NASA is more concerned about protecting this report rather than its own sensitive information. As this hearing demonstrates, this Committee is very aware of the impact of releasing sensitive information. I am worried, however, that NASA is suppressing this report not because it would compromise security but because it would embarrass the agency. Would the NASA Office of Inspector General be willing to conduct a review of the decision to classify this report as sensitive but unclassified?

Ms. ROBINSON. Well, I have to admit I haven't thought of that. We certainly could take it under advisement.

Mr. BROUN. I hope you will do so because I am very concerned about this. And as Chairman of the Oversight Subcommittee, it is my responsibility in our Committee to make sure that we have all the information, and it seems to me that NASA has been more—has let sensitive information out.

Mr. Chairman, I have got a question if you would allow me to go over my time a half-minute.

But, Mr. Keegan, without divulging personal information, how are the individuals that have allowed these compromises been punished, reprimanded, or dealt with? Now, you can tell us that in open session like this. And I realize that also we can go into closed session. We can go into whatever means it takes to protect a personal—a person's identity, et cetera. Certainly I am not asking you to divulge any personal information here today, but can you tell us how have these individuals been reprimanded, punished, or dealt with?

Mr. KEEGAN. Their management has certainly spoken with the responsible individuals about the incidents and the facts underlying the report and I would say taken appropriate personnel action for which the—

Mr. BROUN. Mr. Keegan, that is not an answer. If you would just please—whatever—would you provide that to our Committee or the Committee staff?

Mr. KEEGAN. I don't—I believe as a matter of privacy we can't provide information about employee discipline.

Mr. BROWN. Well, I think you can provide how—individuals, that is true. You cannot tell us how an individual particularly has been reprimanded, punished, or dealt with, but I think you can give us an idea. People need to be reprimanded. What I have seen over and over again in this Oversight Subcommittee, not only in this Committee but others, is people violate what they are supposed to be doing, they violate security, and nothing ever happens. And I am sick of it. And I hope that you all will provide this Committee some information.

Mr. Chairman, my time is expired. Thank you.

Chairman PALAZZO. I now recognize the Ranking Member, Ms. Edwards.

Ms. EDWARDS. Thank you, Mr. Chairman. And thank you to our witnesses today.

You know, when you look back at NASA and the establishment of the Space Act in 1958, it is an important consideration to look at NASA's mission and the complications of balancing both the openness that is expected in the scientific and research innovation community and cooperation around the world with these really important security interests, and so for me it really, you know, raises a question about intent of the agency and the civil servants versus a culture that we need to work to change and shape so that there is more consideration of security, still respecting the overall mission of the agency. And I want to thank the witnesses for their testimony today.

I especially want to commend Ms. Martin. I know that you are here and you are in your waning days after 36 years of public service, and so I want to thank you for that. I am reminded all the time, especially as one who represents a local Congressional District here in the Metropolitan Washington region in Maryland about all of the important and valuable work of our civil servants, wherever they fall.

And so it leads me to the question about what is going on at the agency. And so, Ms. Martin, I would like to address this to you if you would, and other witnesses, please chime in. I wonder if, in looking at the conclusions of your three reports, whether you conclude that the security weaknesses that you found stem from an inconsistent application of policies and guidance on protecting sensitive information, technologies, and other assets of the agency and centers rather than from a conscious disregard of security measures by NASA personnel?

Ms. MARTIN. Well, first, Ms. Edwards, I would like to thank you for your very kind remark, and it is indeed a pleasure to have this opportunity to testify before this Committee, the Subcommittees, a week before I am actually due to retire. It has been indeed an honor and a pleasure to serve the Congress and the American public for 36 years. So thank you very much for that.

And to your question, we certainly did not find any widespread indications of overt attempts to circumvent policies and procedures. As we state in our report, there were certainly some lack of clarity in terms of the policies and procedures, and as you well know, NASA devolves a lot of responsibility to its centers, and so we

found variations across those centers in terms of how they implemented policies and procedures. And no doubt accountability is important, but there was not any widespread indication in terms of our work that someone went about, you know, deliberately trying to circumvent policies and procedures.

Ms. EDWARDS. Thank you very much for clarifying that. And it then leads me, Mr. Webster, to a question for you, and that is around the culture at NASA and what you are doing because it strikes me—and I worked at Goddard Space Flight Center, so I know this—the importance of devolving a lot of responsibilities to the agency because in part that is what creates an environment of innovation and creativity. And so how do you then balance security concerns and preventing breaches of release of sensitive information with a culture in which you want to encourage innovation and creativity? What can you do to bring a lot more consistency to the application of these issues within the agency?

Mr. WEBSTER. I believe that the cultural issue is perhaps one of the largest challenges being faced as a result of this review because unlike information technology or policies that can be changed and so on, changing the culture is a long-term effort. It may be that NASA and the workforce looks at its mission as a set of objectives and then the rest of what NASA has to do is sort of what they have to do in order to be able to execute the mission. And that would be unfortunate. And I suspect that is the case in many cases because instead, the housekeeping types of things that need to occur needed to be viewed as part of the mission so it is not this balancing what do we have to put up with in order to achieve the mission? It is recognized as part of the mission.

And going back to your earlier question, I would say that in my perception, and I believe it is reflected in our study, is that NASA has consistent policy but it is inconsistently applied, and so that is where I think getting the culture to understand that as part of their mission is important.

Ms. EDWARDS. Thank you. Mr. Chairman, if you can indulge me with Mr. Broun's 30 seconds, I would appreciate it.

Chairman PALAZZO. I will.

Ms. EDWARDS. So I want to go to Mr. Keegan. I mean there has been some discussion about an oversight body such as the internal Asset Protection Oversight Board that has been advocated by NAPA to oversee safety concerns. What is your view about the necessity and how NASA would view the necessity of standing up such a board?

Mr. KEEGAN. We think that is a valuable recommendation and we agree that that function would be useful to help us address challenges in this area and we are looking to set up something along those lines that would then report up to the agency's Mission Support Council to implement that recommendation.

Ms. EDWARDS. Thank you very much.

Thank you, Mr. Chairman.

Chairman PALAZZO. I now recognize Mr. Brooks.

Mr. BROOKS. Thank you, Mr. Chairman.

Dick Thornburgh, panel chair, testified before Congress on April the 8th of 2014 that the National Academy of Public Administration, or NAPA, as we have been referring to it, found that "there

is little accountability for noncompliance when identified through specific incidents or periodic assessments. This validates the identified perception among NASA personnel that 'mandatory compliance' means little as there are few if any consequences for deliberate or inadvertent violations of the mandates." NAPA further found that "NASA headquarters officials and center directors have not adequately communicated that strict compliance was and is required for a foreign national hosting, sponsoring, and escort policy and procedures." Finally, NAPA also found that "a number of NASA leaders also noted that the agency tends not to hold individuals accountable even when they make serious preventable errors. Whenever an example of such an error was mentioned during interviews, Academy staff would follow up with: what happened to those responsible for the error? In almost every instance, the answer was either 'nothing' or 'I don't know'." Mr. Keegan, who at NASA is responsible for ensuring accountability for protecting sensitive information at NASA?

Mr. KEEGAN. Ultimately—the ultimate accountability for that is the Administrator and I think the Administrator has made it clear through his actions in response to these reports that he takes that responsibility very seriously. He or the Associate Administrator has traveled to every center to emphasize that every employee has the responsibility in this area. His message that Ms. Martin mentioned earlier that he sent to every employee at NASA said he wanted to—I am quoting—"I also want to remind each of you of your responsibility to comply with all export control regulations and our foreign national management requirements. This is a serious matter and penalties for noncompliance can include fines and imprisonment, as well as administrative personnel actions such as reduction in grade or even termination." And he has directed us, as we improve the internal audit functions for both export control and foreign national access, to address strengthening compliance and accountability mechanisms.

Mr. BROOKS. Well, inasmuch as it is clear that there are many NASA employees who are not doing their jobs protecting NASA's sensitive technology and information or protecting America's national security by protecting information of a national security concern, why haven't these individuals been fired or otherwise seriously punished?

Mr. KEEGAN. I am not sure the specific incidents to which you are referring.

Mr. BROOKS. Well, you just testified that you have got the NASA Administrator, Associate Administrator talking to these individuals who apparently aren't following our sensitive information and national security interest, and that there is a problem in NASA according to the NAPA report. How many of them have been fired, the employees who have not been in compliance with NASA's own rules and regulations concerning protection of sensitive information and protection of our national security?

Mr. KEEGAN. I am not aware of any findings of intentional misconduct on the part of NASA employees but rather problems with understanding the roles and responsibilities as spelled out by the policies and procedures.

Mr. BROOKS. So if the employees are just not doing their jobs, they are not paying attention, they are negligent, grossly negligent, NASA doesn't terminate them because they are doing a bad performance job?

Mr. KEEGAN. We have—we acknowledge that we have shortcomings in this area of accountability and I think the Administrator has taken strong actions to address those shortcomings.

Mr. BROOKS. And does that strong action include the threat to terminate the NASA employees who intentionally or negligently or through gross or reckless misconduct fail to protect sensitive NASA material, thereby also failing to protect America's national security? Do we have assurances that in the future these people will be fired if they risk our country's sensitive information and national security?

Mr. KEEGAN. Well, you have NASA's assurance we will take the appropriate disciplinary actions, the most serious of which include termination.

Mr. BROOKS. Well, I hope in the future that termination will be an option that NASA will utilize because I can assure you in the private sector those folks are gone. And in the public sector we should treat employees who fail to do their jobs similarly. Thank you for your responses.

Chairman PALAZZO. I now recognize Ms. Bonamici.

Ms. BONAMICI. Thank you very much, Mr. Chairman.

Thank you to all the witnesses for your testimony, for being here today. This is an important topic. Of course it has national security implications but also we are pondering whether the recommendations made by the reports that we are discussing here today, whether they could impact some of the core elements of NASA's mission.

Also, I have to say that the public is really looking to us to find the right balance, and we heard that word this morning, balance, quite a lot, between of course keeping our country safe and protecting sensitive research and data, maintaining our country's leadership role, but also understanding that there is importance in NASA publicly disseminating the results of research and the scope of its scientific activities. I have to say that that is important for many reasons but especially to help educate the public about the benefits of NASA's work. So it is finding that right balance.

I do want to point out that, Dr. Webster, you said in your testimony that NASA provided complete cooperation for this review and NASA interviewees were candid, cooperative, and eager to offer both suggestions and be involved in problem-solving, and I just wanted to point that out, that you recognized that when you did your assessment. And that is so important.

We look at the report from the NAPA, National Academy of Public Administration, and they acknowledge that foreign national participation in NASA programs and projects is an inherent and essential element in NASA operations. So considering the implications that the OIG and the NAPA reports have on these areas, I am interested in whether our witnesses see any potential to improve international collaboration through the recommendations of these reports if they are all implemented. Might there be a possibility that international collaboration is improved? If you just want

to each state briefly whether you agree that there is any potential there?

Mr. KEEGAN. I think the thoughtful recommendations from all three of the reports that we are talking about here this morning offer the opportunity for NASA to strengthen its foreign national participation by having clear guidance and by assigning roles and responsibilities that everyone understands and complies with. This will sort of make it easier for involving foreign nationals as appropriate in our research.

Ms. BONAMICI. Does anyone disagree with that? Ms. Martin?

Ms. MARTIN. No. I would agree that it is not an either/or, and obviously foreign participation, international agreements are important to NASA's work, as Mr. Keegan and others have said, but it is important to have those clear policies and procedures and we think that risk-based approach to compliance is really one way that can help NASA with that balance.

Ms. BONAMICI. Ms. Robinson, Dr. Webster, do you agree with—

Ms. ROBINSON. Yes.

Mr. WEBSTER. I do as well. I believe it is a risk-based approach and it is a balancing act. I mean you can obviously have more collaboration by ignoring security, but there is a cost to be paid for that.

Ms. BONAMICI. Right. And thank you. I want to follow up on questions that were just asked. It seems listening to the testimony and reviewing what you have submitted that the core problems described in the reports are because individual NASA employees did not appropriately follow existing policies or procedures. So I want to start with Mr. Keegan. Do you see that as resulting from inadequate training, ineffective organizational structure, or a lack of resources, or some of each?

Mr. KEEGAN. I think that it is a combination, and we are taking action. One of the earlier reports mentioned that there was confusion and bureaucracy in the implementation of these requirements, so we are trying to address that through clarified policy, through clarified training. And also we have detailed a full-time person who is a project engineer who can sort of put these export control requirements in language and in the training sort of in terms of the process that flight project folks understand in terms of what their responsibilities are. So we think there are improvements to be made in all three areas.

And we are allocating, as I mentioned in my opening statement, increased resources to this area as well. And I think the Foreign National Access program will pull together, you know, the coordination of the various elements in this area of responsibility across the agency.

Ms. BONAMICI. And the recommendations that NASA is implementing, do you see those as realistic fixes? Once implemented, will they resolve the problems that were brought to light by the assessment?

Mr. KEEGAN. Absolutely realistic fixes and we hope they will address all of the issues, but in my 32 years at NASA I have never seen a strong external review that has failed to identify some areas where we could continue to improve as well.

Ms. BONAMICI. Thank you.

And I yield back the balance of my time. Thank you, Mr. Chairman.

Chairman PALAZZO. I now recognize Mr. Posey.

Mr. POSEY. Thank you, Mr. Chairman.

Mr. Keegan, I think you are aware everybody on this panel, probably everyone in this room I think is a friend to NASA. They recognize NASA does many wonderful things. They want them to do many more things. But like everybody in this room, NASA is not perfect. We can't expect anybody to be perfect. But we are talking about matters of national security now and we need to be as close to perfect as we can possibly be. And when Members ask questions like about disciplinary action in the past, you know, and they kind of get rope-a-dope here, you know, the bobbing and weaving, no direct answers. It sounds petulant, arrogant, defiant. It seems like an us-against-them, and I know that you don't intend that but that is how it comes across.

This is not my first rodeo with issues like this. Financial Services Committee, the Securities and Exchange Commission played rope-a-dope with us for a couple years. They let Bernard Madoff steal \$70 billion from people, innocent people. People died because of it. People went broke. People are living in poverty now instead of a comfortable retirement because about 50 people in that agency didn't do their job. And we had great Inspector General reports, IG reports, made recommendations about what the accountability should be, and we got the rope-a-dope from the SEC for years. Well, we are working on it. Some of these things are still pending. We can't talk about them. It is a big secret.

So finally, basically under Freedom of Information Act, we find out that none of the recommendations for disciplinary actions were taken. Everybody was let off easy. One explanation that was supposed to make us happy is the Secretary said, well, it might please you to know that half the employees are no longer with the agency that let him do all these things bad. I said, well, you know, great. That is problem solved. A pedophile moved into a different neighborhood. No. I mean they are retired on the government's dime. They took jobs as investigators or compliance people for other agencies maybe. That doesn't solve any problems because they are not with the agency.

So we wonder how many of people in your agency that we are going to find out three years from now, oh, well, we let them hang in there until they got a better job and could double their salary on K Street or whatever, you know. I mean we would like some serious answers and I think you owe them.

And my question to you now, has any disciplinary action ever been taken? And you can tell me yes or no and tell me what kind it was.

Mr. KEEGAN. Yes, disciplinary action has been taken. I know certainly of instances of counseling. I don't know of—

Mr. POSEY. Okay.

Mr. KEEGAN. —any other specifics related to the issues in these reports we are talking about here today. I certainly know about instances elsewhere in NASA where—I mean I don't think NASA shies away from taking appropriate discipline up to and including removal.

Mr. POSEY. Has anyone ever been removed, do you know?

Mr. KEEGAN. At NASA?

Mr. POSEY. Yes, sir.

Mr. KEEGAN. Sure.

Mr. POSEY. Over security breaches?

Mr. KEEGAN. I don't know that.

Mr. POSEY. Could you find out for us? We would like to kind of have a summary. You can tell us what actions have taken and you don't have to name employees. The IG has even named specific employees and said this employee did this; they should be disciplined like such. Of course they weren't, you know, but I think we would like to know what the history is, with the track record is, if actions have really been taken. I mean do these people write these reports to come in and give them to Congress and then the agencies just blow them off and say, those suckers, they can't make us do anything?

I mean that is the way it seems sometimes. That is the way a lot of the taxpayers feel at home. They see that there is a lack of accountability in government. We come here, we hold hearings, and yeah, we will check into that, yeah, we will report on that, and sure, we will get back with you. But we don't. I mean I have got stacks of unanswered correspondence, you know, over my head. It seems like, you know, some of the agencies just refuse to do any compliance and it just—it seems like it is us, government, against them, the public or their representatives. And we would like to think that that culture is not pervasive in NASA, but when we can't get straight answers, that is the conclusion people tend to think. And it makes it hard.

I mean we want to get funding for NASA to big things. It takes money. And the public perception is, you know, that NASA gets 20 percent of the budget. We know the reality you get 1/2 of one percent and we know that is plundered. We know that comes through like a big pinata from everything from the COPS program to whatever other pet projects people want to steal from NASA because, number one, we don't do a good PR job in NASA and I could spend a couple hours talking about that; and number two, people already think we spend too much money on it; and number three, there is cases like this where they don't see a lack of accountability.

So I would hope that when you come in here to share with us, we work toward changing that, that it is not us against them. We are just trying to see that there is some fundamental accountability. We try and teach our children that in school. You know, everybody in the private sector has it that I know about and we just want to see that that is in place at NASA, too.

And again, we are not talking about personalities. We are literally, we are literally talking about the national security of this Nation. We are talking about people that come here from another country and we can't expect you to profile everybody who is going to have access to any information because they shake down everybody when they get home, from tourists, to students, to everybody else. We know that is tough but we have to get off the dime and move in that direction. And when people seemingly almost willfully violate or transgress guidelines that make this nation secure, they

need to be held accountable and you need to let us know that that is happening.

Thank you, Mr. Chairman. I yield back.

Chairman PALAZZO. I now recognize Mr. Johnson.

Mr. JOHNSON OF OHIO. Thank you, Mr. Chairman.

I would like to associate myself with some of the comments that my colleague Mr. Posey said. I am a big fan of NASA. I mean I grew up on Buck Rogers and Star Trek and enamored by space travel. I have got NASA, Glenn, in Ohio. I am a big, big fan of NASA's.

But, Mr. Keegan, some of your responses don't rise to the level of credibility with what we are dealing with here today. How did you go about preparing for this hearing today? You knew this was going to be about security breaches and personnel having done those, but we are getting a lot of "I don't know" answers. What did you do to prepare for today's hearing?

Mr. KEEGAN. I reviewed the reports and—

Mr. JOHNSON OF OHIO. You did review the reports?

Mr. KEEGAN. Yes.

Mr. JOHNSON OF OHIO. Okay. That is a good start because you said earlier that you were not aware of any deliberate actions by NASA employees to violate security protocols. Have I got that right? Is that what you said earlier?

Mr. KEEGAN. I am not aware of any specific employees that have—

Mr. JOHNSON OF OHIO. Okay. Well, in the report—

Mr. KEEGAN. —been identified—

Mr. JOHNSON OF OHIO. —from—in the report from GAO they state that in some instances in terms of trying to avoid export control review, they said it was the result of deliberate action by authors to avoid export control review of papers prior to release. And yet you say you read the reports and to come to this hearing and not know whether or not people have been addressed and disciplined for those types of deliberate actions, that doesn't rise to a level of credibility for me, and I worked for almost 26-1/2 years in the Air Force, much of that in top-secret and classified conditions. I know at least in the environment I worked in where the buck stopped. You are pretty close to where the buck stops. I am a little incensed that you don't know the answers to these questions that you are saying you don't know the answers to.

Let me go back to one that Mr. Posey asked you. You said that there have been people removed from NASA but specifically in your written testimony you noted that penalties for noncompliance with export control regulations, of which reviews are part of and Foreign National Access Management requirements, that those penalties could include fines, imprisonment, or administrative personnel actions. Well, let me ask you again—and you don't have to give me a specific name of anyone—but do you—has anyone in NASA received any of those things—fines, imprisonment, or administrative personnel actions—for a security breach—for a deliberate security breach, as noted by GAO? Has anyone been disciplined to that level?

Mr. KEEGAN. I will take that question for the record and provide you a response.

Mr. JOHNSON OF OHIO. Okay. I would appreciate that. Thank you very much.

Ms. Robinson's testimony noted that NASA's Jet Propulsion Laboratory has had success using engineers and scientists as export control representatives to work with the export control personnel, so I will ask, Mr. Keegan, if you know the answer to this. Maybe others on the panel want to comment. Can someone provide a more detailed explanation of the process of working with scientists as export control representatives? I mean what do the scientists at NASA's Jet Propulsion Laboratory do that scientists at NASA centers do not do? How do they work differently with export control personnel?

Mr. KEEGAN. I would like whoever reviewed that as a model that we can look at to describe it.

Mr. JOHNSON OF OHIO. Okay. So we are not sure. Okay.

Ms. ROBINSON. I think it is just—again, this was not in our report; it was something that I noted in the other reports, but I think it is a process that they have in place, a way to have interactions between the two groups of professionals so they are having conversations and they are understanding what kind of projects are we working on, are there foreign nationals working here, how do we resolve these issues? So it is a process.

Mr. JOHNSON OF OHIO. Okay. All right. Well, that five minutes went fast.

Mr. Chairman, I guess I will yield back the balance of my time, the one second I have got.

Chairman PALAZZO. Are you sure you don't want 30 more seconds or a minute? Okay.

That is perfect time and I do believe votes were just called or did they go back in session? Well, the buzzer went off.

Well, it is absolutely obvious that this Committee takes our national security very importantly. It is a bipartisan issue. It is also obvious that when you look at the global events around the world that the world is not becoming safer; it is becoming much more dangerous. And America's leadership in space isn't just about national pride; it is about national security. And we are not going to wait 15 years to make sure that these recommendations are being implemented by NASA. We are going to be looking forward to reports every year and we are going to be taking a hard look at this.

So I thank the witnesses for their valuable testimony and the Members for their questions. Members of the Committee may have additional questions for you and we will ask you to respond to those in writing. The record will remain open for two weeks for additional comments and written questions from Members.

The witnesses are excused and this hearing is adjourned. Thank you.

[Whereupon, at 11:22 a.m., the Subcommittees were adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Richard Keegan

Questions For the Record

From Ranking Member Donna F. Edwards

"NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information"

To Mr. Richard Keegan

QUESTION 1:

Your prepared statement refers to a NASA submitted legislative proposal that you state would, if adopted, "authorize NASA to withhold from public disclosure certain technical data with aeronautic or space application from release under the Freedom of Information Act (FOIA) if such data may not be exported lawfully outside the United states without an approval, authorization, or license under the provisions of the Export Administration Act (EAA) of 1979 or the Arms Export Control Act (AECA) of 1976."

- a) Could you describe the problem that this proposal addresses at NASA?
- b) Why aren't existing FOIA exemptions sufficient?
- c) Is this proposal a preventative measure, or is NASA being requested to make FOIA releases of information that is export-controlled and for which NASA is unable to get an exemption?

ANSWER 1:

NASA receives FOIA requests every year for export-controlled technical data with aeronautics or space application. As noted in the prepared statement, there is at present no particular exemption in the FOIA that directly applies to such information, nor is there any statute that specifically allows NASA to withhold it from release under FOIA. Therefore, NASA is forced to attempt to use available exemptions, often not ideally suited for the circumstances, in order to prevent public release of the information under FOIA. While thus far NASA has been able to apply existing exemptions to FOIA requests, it may not always be able to do so defensibly. The requested statutory authority would put NASA on par with the Department of Defense which, through 10 USC 130, is able to withhold the very same information which NASA creatively tries to protect, and provide NASA with the same clear and predictable approach to dealing with FOIA requests for export-controlled information. NASA's proposal is in fact modeled after the DoD statute.

QUESTION 2:

Can NASA apply all of the actions recommended by the NASA OIG, GAO, and NAPA within the current level of funding it has been given for these activities by Congress? Are there potential unintended consequences of organizational changes as recommended by NAPA? Could NAPA's recommendation to realign Special Agents to report to their respective Center Directors be one of those potential unintended consequences? If so, why?

ANSWER 2:

NASA has provided additional funding to enhance the Foreign National Access Management and Export Control Programs and has re-assigned additional Federal personnel to support the development of training and documentation to support these programs.

NASA concurred with the intent of NAPA's finding to increase integration of the Counterintelligence Special Agents (CISAs) at the Centers, but not with the recommended implementation of decentralizing the program. A decentralized Counterintelligence (CI) program has proven ineffective at NASA; however, NASA recognizes the need to improve Center personnel access to their CISA and the benefit of increased integration into Center operations. At each NASA Center, the CI Office is required to have a quarterly meeting with the Center Director. During these meetings, the Center Director is brought up to date on any counterintelligence or counterterrorism matters affecting the Center. In addition to the quarterly meetings the Counterintelligence officials meet with the Center Director on an as needed basis. At Headquarters, the Assistant Administrator for Protective Services, NASA's senior counterintelligence, security and intelligence official, provides monthly CI/Security briefings at the Agency level Senior Staff meetings, which include the Officials in Charge at NASA Headquarters and NASA Center Directors. In addition, at Headquarters, the CI Division Director meets with the Administrator and Associate Administrator on an as-needed basis to brief them on counterintelligence and counterterrorism matters affecting the Agency. NASA is increasing the awareness of all employees and leaders across the Agency.

QUESTION 3:

In his response to the NAPA report, the Administrator said that he has asked the Associate Administrator for International and Interagency Relations to review the panel's recommendations and provide an assessment of additional resources that may be required to successfully implement the proposed recommendations. What is the status of this review? When will it be completed, and will any changes in resource allocation be reflected in an updated Operating Plan?

ANSWER 3:

NASA has provided additional FY 2014 funding to the Export Control Program and temporarily re-assigned additional Federal personnel to support the development of an Export Control Program Manual and a major revision of NASA's Export Control Training Program. Both of these activities were recommendations from the NAPA report.

NASA has also secured commitments from the State Department and Commerce Department to provide advice and review drafts of the manual and training material. NASA will continue to work closely with the regulatory agencies to improve the

efficiency and effectiveness of the NASA Export Control Program and ensure continued compliance with these laws and regulations.

With this additional funding, additional Federal personnel, and commitments from our regulators, NASA believes we have sufficient resources to address the export control recommendations from the NAPA Report.

QUESTION 4:

Why has NASA, as reported by NAPA, not utilized detailed policies and procedures regarding comprehensive approaches to asset protection that have been implemented by other federal agencies such as the Department of Energy?

ANSWER 4:

NAPA indicated that there are enough similarities between NASA and DOE to warrant assessment of possible application of procedures, training, and oversight regarding foreign visitors to NASA. The Foreign National Access Management program will be engaging stakeholders at all levels and reach out to other agencies, including DOE, to discuss common challenges.

QUESTION 5:

NAPA found that although NASA directives state that compliance is mandatory and accountability is established, there appears to be little accountability for noncompliance. NAPA said NASA personnel perceive "mandatory compliance" as meaning little since there are few if any consequences for deliberate or inadvertent violation of the mandates. How is NASA addressing this perceived absence of accountability?

ANSWER 5:

The protection of sensitive technologies is the personal responsibility of all NASA employees and a responsibility that every NASA manager, right up to and including the Administrator himself, takes very seriously. Indeed, in May, Administrator Bolden directly addressed those officials from across the Agency who manage the implementation of NASA's Export Control Program about the critical role they play in safeguarding sensitive NASA technologies. He also issued a communication to all NASA employees reminding them of their responsibility to comply with all export control regulations and foreign national access management requirements. His message stressed that safeguarding sensitive information is a serious matter and that penalties for noncompliance can include fines and imprisonment, as well as administrative personnel actions, such as reduction-in-grade or even termination. The Administrator also encouraged employees to meet with their local export control officials to learn more about NASA's Export Control Program and their responsibilities in protecting sensitive technologies. We will elevate the visibility of compliance accountability through functional reviews and employee performance standards. From the Agency's top

management down to its newest employee, we are redoubling our efforts to perfect export control compliance through enhanced communication and training, ensuring all employees know their roles in this effort and the consequences if they do not comply with Agency regulations and Federal laws.

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON SPACE
SUBCOMMITTEE ON OVERSIGHT

"NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information"

Questions for the Record, Mr. Richard Keegan, Associate Deputy Administrator,
National Aeronautics and Space Administration (NASA)

Questions submitted by Rep. Steven Palazzo, Chairman, Subcommittee on Space and
Rep. Paul Broun, Chairman, Subcommittee on Oversight

QUESTION 1:

The GAO report stated, "We identified instances where NASA security procedures for foreign national access were not followed, which were significant given the potential impact on national security or foreign policy from unauthorized access to NASA technologies. Specifically, at one center, export control officials' statements and our review of documentation showed that, in seven instances between March and July of 2013, foreign nationals fulfilled the role of sponsors ... by identifying the access rights to NASA technology for themselves and other foreign nationals for one NASA program."

- a. Has anyone been held accountable for these violations of NASA security procedures? If so, how?

ANSWER 1:

NASA is committed to reviewing recommendations by independent evaluators such as the General Accountability Office (GAO) and to having those evaluations inform changes in the Agency's existing processes in order to better safeguard access to NASA facilities by foreign nationals and to improve the protection of sensitive technologies. The referenced GAO report as well as other recent independent investigations into export control and foreign nationals access management processes have the Administrator's personal attention and he has ordered a series of changes, to include increased employee accountability, revised Agency policies and procedures and improved employee training so as to prevent incidents like this from happening again.

The protection of sensitive technologies is the personal responsibility of all NASA employees and a responsibility that every NASA manager, up to and including the Administrator himself, takes very seriously. Therefore, in May 2014, Administrator Bolden directly addressed those officials from across the Agency who manage the implementation of NASA's Export Control Program about the critical role they play in safeguarding sensitive NASA technologies. He also issued a communication to all NASA employees reminding them of their responsibility to comply with all export control regulations and foreign national access management requirements. His message stressed that safeguarding sensitive information is a serious matter and that penalties for

noncompliance can include fines and imprisonment, as well as administrative personnel actions, such as reduction-in-grade or even termination.

It is important to note that the recent independent reviews conducted by the GAO, the National Academy of Public Administration (NAPA) and NASA's own Inspector General's Office did not identify any instances when NASA employees maliciously bypassed export-control restrictions, thereby violating Federal laws, nor did they document any occurrences of NASA employees purposefully sharing sensitive information with foreign nationals. Instead, the independent reviews identified instances of employee carelessness and poor judgment with respect to export-control and foreign national access procedures at NASA Centers, which led to policy and procedural violations. These findings resulted mostly from employee confusion regarding individual roles and responsibilities in the export control and foreign national access management process. Given this confusion, Administrator Bolden directed Associate Administrator Lightfoot to assess these independent review findings and to recommend any potential corrective action in terms of Agency policies and procedures with regard to these findings. Additionally, instances of alleged violation of Agency policies by specific NASA employees have been and will be handled administratively using established disciplinary processes.

QUESTION 2:

The GAO report stated that "Federal internal control standards highlight the importance of managers developing plans with specific timeframes and comparing actual performance to expected results; however, only two centers developed timeframes for completing actions and only one had developed plans for assessing the effectiveness of actions taken." Further, the report stated that, "Without plans and timeframes to monitor corrective actions, it will be difficult for NASA to ensure that actions are implemented and effectively address foreign national access related issues."

- a. Why hasn't NASA required a timeframe for implementing corrective actions?

ANSWER 2:

NASA strives to complete corrective actions expeditiously. Consistent with recommendations from the GAO, NASA is revising its policies on the annual Export Control Program (ECP) audits to specify that Center Directors shall oversee the completion of the annual ECP audits and report their implementation or progress to the Associate Administrator for International and Interagency Relations (OIIR) and to the NASA Headquarters Export Control Administrator (HEA). Audit findings and progress towards corrective actions are also an input to the Integrated Functional Reviews conducted by various Headquarters offices at the Centers. Progress (or lack of progress) towards open actions is also reported in the annual ECP audits. Including Center Directors and the Associate Administrator for OIIR in the responsibility chain for implementation and monitoring of corrective actions provides increased senior management attention that will ensure that actions are implemented and effectively addressed.

NASA used a risk-based prioritization of the NAPA recommendations in preparing implementation actions associated with the Agency's responses to those recommendations, and will initially focus on those recommendations involving the highest risk. Accordingly, NASA established the Foreign National Access Management Program on March 10, 2014. This program is an ongoing effort to coordinate and strengthen NASA's foreign national management and export control policies and practices. NASA established a foreign national access management-working group in May 2014 and executed a program commitment agreement between the Office of Protective Services, OIIR, and the Office of the Chief Information Officer in June 2014. The Foreign National Access Management Program Manager developed a systematic approach to accomplishing an inherently complex mission that will require coordination of three distinct Agency offices and stakeholders at all levels across the Agency. A draft program schedule identifying tasks supporting the execution of identified corrective actions from FY 2014 through FY 2018 has been developed and is undergoing broader Agency review.

QUESTION 3:

Scientific and Technical Information (STI) that is intended to be released outside of NASA is required to be reviewed in order to ensure it does not include sensitive information. The GAO report stated, "Based on our review of NASA's most recent STI compliance audits, most centers continue to release STI that has not been reviewed for export control purposes." GAO also found that 20 percent of released information was not reviewed. GAO went on to state, "We did not assess STI documents that were not reviewed or information that was posted on NASA websites without export control review to determine if their release violated export controls, but without the completion of these reviews, NASA is at increased risk of inadvertently releasing controlled technologies."

- a. What is NASA doing to ensure that it is not releasing sensitive information?

ANSWER 3a:

NASA takes the responsibility of securing sensitive and export-controlled information at its facilities and within its information technology (IT) systems very seriously and is working to implement all of the recommendations from several external audits and reviews. Recognizing the growing threat aimed at Government agencies by hostile nation-states and foreign adversaries, the NASA Administrator has already directed a number of actions to further secure sensitive and export-controlled information at NASA facilities and within its Information Technology (IT) systems and to enhance overall security.

NASA appreciates independent reviews of our programs and policies, and we are committed to reviewing recommendations made by those independent bodies and to having them inform changes in the Agency's existing processes in order to better

safeguard sensitive technologies and data maintained by the Agency. For example, the GAO report published in April 2014 complements recent reviews conducted by the NASA Office of Inspector General (OIG) and the National Academy of Public Administration (NAPA), which provided its findings to the NASA Administrator in January 2014. NASA's responses to the GAO, OIG, and NAPA recommendations are assisting in our continuing efforts to enhance all aspects of our foreign national access management, information technology security, access to sensitive information, and NASA's export control compliance program. The GAO report made seven recommendations to the NASA Administrator intended to ensure consistent implementation and improve oversight of NASA's export control program. NASA has accepted all seven of these recommendations and is in the process of implementing those recommendations.

Additionally, recent IT improvements by the NASA's Office of the Chief Information Officer include:

- The CIO has significantly enhanced the Agency's ability to monitor activity on our networks (Trusted Internet Connections (TIC), Intrusion Detection Systems, Intrusion Prevention Systems, web content filters, etc.).
- We have increased collaboration with other Federal agencies to share intelligence on threats and vulnerabilities (DHS, FBI, NSA, established Threat Management Cell, etc.).
- We are continually adjusting our tools and procedures at the Agency and Center level to the changing threat environment to better protect our information, detect anomalous activity, and mitigate incidents (Web Applications Security Program, PIV Mandatory, Continuous Diagnostics and Monitoring, etc.).
- We are in the process of transforming our network architecture to address the challenges of protecting sensitive technical information, yet openly sharing other types of information with the public and our partners (network zoning, network access control, WESTPrime, cloud computing, etc.).
- We are improving the collaboration across the programs to integrate security into the System Development Lifecycle (static code analysis, web vulnerability scanning, Space Asset Protection Working Group, etc.).
- Additionally, NASA conducts a yearly Scientific and Technical Information (STI) Compliance Review to ensure that the NASA Centers appropriately use the existing STI policy when posting information to Agency websites. This review tracks two measures: 1) How frequently STI documents are correctly processed; and, 2) Whether identified documents have been properly reviewed prior to release or publication. The results of measure 1 for the last audit year (2012) showed 96 percent compliance across all Centers – an increase of 2 percent from 2011. The results of measure 2 for 2012 showed 84 percent compliance – an increase of 4 percent from 2011. Based on the 2012 results, the following improvements are being made Agency-wide*:
 - Agency system (ongoing): Based on available resources, STI is continuing to roll out an Agency electronic system to review and approve STI to standardize submissions (and insight into them) across the Agency vs. Center by Center.

- STI Awareness (ongoing): Communication plans have been required by all Centers to continue to inform authors of their responsibilities and process to review and approve their STI.
- Center Directors Follow-up (new): Direct involvement is being requested from Center Directors' offices in awareness and compliance activities at their Centers. Center Directors should respond in writing to these audits to the Agency CIO. Additionally, Center management has reinforced the requirement for export control review in advance of any release or publication, and the CEA reports a dramatic reduction in such deliberate actions.
- Continued monitoring of Centers (new): monthly/quarterly spot-checking of third-party sources in which NASA STI may be announced (open literature, etc.) and follow-up with non-compliant authors through the Centers.
- Specific possible gap analysis (new). STI is recommending to the Agency CIO to establish an Agency "red team" to better understand and fix any gaps related to STI being loaded to websites without STI review. This team would include STI, Export Control, and Web Services representatives and report back to the Agency CIO.
- Specific cases (new): Any Centers with downward trends in these measures or lower than typical scores are asked to increase their awareness at their Centers. STI will monitor these Centers more closely.
- Note: 2012 is the last full-year information available at this time. The 2013 audit work was delayed due to the sequestration budget impacts and due to NASA taking the NASA Technical Report Server offline temporarily while a detailed export-control review of associated documents was conducted. NASA is working on the 2013 audit information now.

QUESTION 3b:

In some instances GAO noted that this was a result of " ... deliberate action by authors to avoid export control review of papers prior to release." It appears as though NASA is both negligent in failing to review the release of information and in some instances employees are actively working to avoid reviews. What is NASA doing to reprimand those that attempt to violate federal regulations? How many individuals has NASA reprimanded for this behavior?

ANSWER 3b:

The GAO's reference to a "deliberate action by authors to avoid export control review" came from a routine Agency review of security procedures performed by the Office of Protective Services (OPS). Thus, NASA was aware of the procedural lapses and was already taking corrective action prior to the reference in the GAO report. Once discovered, the referenced Center took several actions to increase the number of personnel conducting reviews prior to release and to establish processes to report individuals that do not follow established processes to their respective supervisors for appropriate action.

To be clear, the infractions identified in the GAO report represented noncompliance with NASA procedures and were not violations of law, including the Export Administration Regulations or the International Traffic in Arms Regulations. Such infractions of Agency policy are addressed administratively, using established disciplinary processes. (Please see response to Question 1.)

QUESTION 4:

Ms. Martin's written testimony stated that NASA's procedural requirements for Scientific and Technical Information requires that all STI intended for release outside NASA or presented at internal meetings where foreign persons may be present must undergo technical, legal, and export control reviews?

a. How does this currently take place? How much time does it take?

ANSWER 4a:

NASA uses a standard process, called the Document Availability Authorization (DAA), to conduct reviews and provide approvals for STI that will be released, published, or disseminated external to NASA or made available in situations in which foreign persons are present. The reviews determine if the STI is publicly available or must be restricted or limited. If restricted and limited, the DAA process indicates who may access the STI. NASA is in the process of phasing-in an electronic DAA to streamline routing of review packages and better track the process. Processing times vary, depending on the complexity and length of the information being reviewed. NASA requires at least two weeks advance notice before presentations are to be given. Longer lead times are required for articles, publications, or books.

QUESTION 4b:

Do NASA project personnel have concerns with this process?

ANSWER 4b:

As with any process, improvements can always be made. NASA is cognizant of the concerns about the STI process expressed by users, to include some confusion about the definition of STI vs. non-STI and user suggestions for streamlining the STI review process as a whole. NASA is working to make the process friendlier for users, while also ensuring that the Agency complies with all Federal laws regarding required export-control review of STI-related material.

QUESTION 4c:

What recommendations would you suggest to accommodate NASA project personnel's concerns while still accomplishing the needed reviews?

Answer 4c:

Some examples of changes NASA has made to address project personnel concerns are:

- NASA has established a Blanket DAA process with the Agency Export Control Administrator (ECA). This allows, after determination by the Project or Program officials and ECA, a faster process to review fundamental research documents with fewer approvals.
- STI will be undertaking a reengineering project related to the DAA to determine if any of the complex workflows can be removed or simplified. However, there is one caveat, which is that most of this review is currently based on Federal law, so simplification in many areas will not be possible unless US Statutes are changed.
- STI has implemented a DAA Configuration Management Board for collecting and responding to concerns about the Agency system and clarifying processes and procedures
- Additionally, consistent with a recommendation from the GAO Report, NASA will evaluate resource requirements for the CEA function at each Center. In parallel, NASA is working with each of the NASA Centers to confirm current resource allocations and solicit specific concerns regarding workload-related issues. Last year, NASA completed a Lean Six-Sigma review of the workload and workflow associated with a CEA position at one Center in order to evaluate resource requirements. NASA will incorporate lessons learned from that review to shape the evaluations of resource requirements at other Centers.

Question 5:

The Committee is aware of allegations of "venue-shopping" in order to gain permission to release sensitive information. When a request to release information is turned down by one reviewing official, the requestor will simply ask someone else either in the center or at headquarters until they get approval.

- a. How much contact do Center Export Administrators have with one another? What opportunities do you see for improving NASA's security through collaborative work by Center Export Administrators at Centers and headquarters to prevent "venue-shopping?"

ANSWER 5:

While we cannot confirm the allegations of "venue-shopping," NASA has implemented a number of processes and practices to ensure greater consistency in export control compliance. CEAs are encouraged to communicate with one another frequently on large, multi-Center programs and projects. Additionally, the HEA holds quarterly videoconferences with CEAs and Center export control staff to discuss issues, identify concerns, and share best practices regarding the implementation of NASA's Export Control Program.

In response to a recommendation from the NAPA review, NASA is developing an Export

Control Program Manual that will provide standardized processes for export control activities and a central location for best practices and information related to implementing the Export Control Program. This manual will facilitate consistent application of NASA requirements and the export control regulations that it enforces.

At the most recent annual Export Control Program Review in May 2014, the HEA briefed the CEAs on a new process to document and report on actions and issues raised by CEAs. Issues and comments were documented by support staff and merged into actions. The HEA assigned due dates for each action and will report on progress during the quarterly videoconferences with the NASA Export Control Program community. Participants will have the opportunity to raise additional concerns or issues during the videoconferences. As appropriate, these issues will also be adopted for action, and reviewed at future videoconferences. This approach will establish a continuous process for CEAs and other NASA Export Control Program professionals to raise issues and understand the progress on their resolution to communicate more frequently and consistently, and to reduce the likelihood for perceptions of "venue-shopping." This process for continuous improvement will be documented in the Export Control Program Manual that is currently in development.

QUESTION 6:

The OIG's reports regarding Langley and Ames point to a great deal of confusion regarding the roles, responsibilities, and requirements for contractors -particularly in instances where NASA Centers house non-governmental "institutes" like the National Institute of Aerospace (NIA) at Langley. The IG's report on Jiang stated, "NIA appeared to lack sufficient procedures to ensure that appropriate officials in its organization were informed of the restrictions NASA placed on Jiang's access to the Center [Langley]."

- a. How can NASA and contractors prevent foreign nationals from slipping through the cracks and obtaining inappropriate access to NASA IT resources and facilities?

ANSWER 6:

NASA's successful accomplishment of its mission requires a diverse workforce and cooperation with international partners. NASA takes safeguarding its facilities and information seriously. There is a single Agency process for granting foreign nationals access to NASA facilities or information technology resources. NASA evaluates foreign national access on a case-by-case basis in accordance with the Agency process to ensure all security, export controls, and information technology policy and procedure are applied and followed.

NASA recognizes the need to strengthen foreign national access management policy and procedure to ensure compliance and accountability. In March 2014, NASA established the Foreign National Access Management Program. This program will focus on: (1) providing consistent guidance, training, and oversight across all NASA Centers; (2) engaging all stakeholders in the identification of best practices and creation of operational

manuals and materials; and, (3) incorporating stronger compliance and accountability mechanisms into NASA's existing Center Integrated Security Functional Reviews.

QUESTION 7:

One of the problems illustrated in the NASA Office of Inspector General report on Bo Jiang is that having too many layers of bureaucracy involved in foreign national access management may negatively affect enforcement of restrictions. What specific recommendations do you have for standardizing and streamlining the process of screening foreign national visitors across centers?

ANSWER 7:

NASA's successful accomplishment of its mission requires a diverse workforce and cooperation with international partners. NASA takes safeguarding its facilities and information seriously. There is a single Agency process for granting foreign nationals access to NASA facilities or information technology resources. NASA evaluates foreign national access on a case-by-case basis in accordance with the Agency process to ensure all security, export controls, and information technology policy and procedure are applied and followed.

NASA recognizes the need to strengthen foreign national access management policy and procedure to ensure compliance and accountability. In March 2014, NASA established the Foreign National Access Management Program. This program will focus on: (1) providing consistent guidance, training, and oversight across all NASA Centers; (2) engaging all stakeholders in the identification of best practices and creation of operational manuals and materials; and, (3) incorporating stronger compliance and accountability mechanisms into NASA's existing Center Integrated Security Functional Reviews.

QUESTION 8:

The OIG report on Bo Jiang describes a list of 32 provisos that can be attached to a foreign national's request for access to a center. The report noted that many employees, even in the Export Control office, did not understand some of the provisos but applied them nonetheless. For example, Jiang's plan included the proviso "The visit is approved based on no cost to NASA; payment of stipends/expenses against a NASA grant/contract/agreement is not authorized," despite the fact that Jiang was to be paid as a NASA contractor.

- a. Who is responsible for writing and updating the provisos if even NASA's export control staff does not understand what they mean?
- b. Would the system be more effective with fewer provisos that were more strictly applied?
- c. Are there any provisos that you think should be discarded?
- d. Are there any provisos that you think should be added?

ANSWER 8:

Provisos that limit or define access to NASA facilities or systems can be prepared by the Center, the Program, or the Headquarters organization participating in the review including the Office of the Chief Information Officer, the Office of International and Interagency Relations and the Office of Protective Services. NASA has established a Foreign National Access Management Program that will coordinate the implementation of NASA policies for foreign national access and is preparing a Foreign National Access Management Program Manual to provide standard guidance on the review of requests for access. We will review our existing set of provisos to see if they could be simplified or if the wording could be clarified.

QUESTION 9:

Mr. Webster's testimony noted that too much flexibility in a procedural process, coupled with a "stove piped" organizational structure such as NASA's, can create inconsistency and poor outcomes. Which aspects of foreign national access management and export control require flexibility in decision-making? Which aspects are best conducted with a more rigid process?

ANSWER 9:

NASA's Export Control Program and our Foreign National Access Management Program have been consistently evolving to address technology transfer and security challenges. For example, we are presently working to revise and consolidate the Security and Technology Transfer Control Plans that govern access to our facilities by certain foreign nationals, and we have appointed a new Foreign National Access Management Program Manager to oversee the implementation of additional improvements in that program. The Foreign National Access Management Program is a collaborative effort between the Office of Protective Services, the Office of the Chief Information Officer, and the Office of International and Interagency Relations. These offices are collaborating on policy review, procedure updates, and the creation of a Foreign National Access Management Manual and an Export Control Manual. The enhancement of policy, procedure, and training resources are the result of implementing recommendations from the GAO, NAPA, and our Inspector General.

QUESTION 10:

Are there any security guidelines that NASA should consider eliminating? Are there any security guidelines that NASA should consider adding?

ANSWER 10:

NASA's Export Control Program and our Foreign National Access Management Program have been consistently evolving to address technology transfer and security challenges. For example, we are presently working to revise and consolidate the Security and

Technology Transfer Control Plans that govern access to our facilities by certain foreign nationals, and we have appointed a new Foreign National Access Management Program Manager to oversee the implementation of additional improvements in that program. The Foreign National Access Management Program is a collaborative effort between the Office of Protective Services, the Office of the Chief Information Officer, and the Office of International and Interagency Relations. These offices are collaborating on policy review, procedure updates, and the creation of a Foreign National Access Management Manual and an Export Control Manual. The enhancement of policy, procedure, and training resources are the result of implementing recommendations from the GAO, NAPA, and our Inspector General.

QUESTION 11:

The OIG report on Ames stated that there was "significant disagreement between scientists and engineers at Ames and export control personnel at the Center and NASA headquarters as to whether the work the foreign nationals were performing... involved ITAR controlled technology." Similarly, the GAO found that "NASA lacks a comprehensive inventory of export-controlled technologies and is not fully utilizing oversight tools." It appears as though NASA doesn't even know what information it needs to protect.

- a. Who is responsible at each center and at headquarters for cataloging ITAR and export-controlled information?

ANSWER 11:

Each Center has a CEA appointed by the Center Director, responsible for assessing and ensuring compliance of all Center program activities with U.S. export control laws and regulations. In addition, each Center has an Export Counsel, appointed by the Center Chief Counsel and responsible for providing legal guidance to the CEA in NASA export control matters under the EAR, the ITAR, and other applicable regulations. Ultimately, Center Directors are responsible for ensuring that all projects under their purview comply with U.S. export control laws and regulations and NASA requirements.

The HEA is appointed by the Associate Administrator for International and Interagency Relations and is responsible for assessing and ensuring compliance of all NASA program activities and exports with U.S. export control laws and regulations. The HEA is also NASA's policy and licensing liaison with the U.S. Government's export control community. Additionally, the Headquarters Export Counsel is appointed by the General Counsel and is responsible for providing legal guidance to the HEA in NASA export control matters under, among others, the EAR and the ITAR. Ultimately, the NASA Administrator is responsible for ensuring that all NASA programs and projects comply with U.S. export control laws and regulations and NASA requirements.

In addition, consistent with the recommendation in the GAO and NAPA Reports, NASA will implement a risk-based approach for targeted technologies of particular concern, working with CEAs, program managers, and counterintelligence

professionals to identify key technologies and catalog those key technologies at each Center. NASA has committed to develop an export control manual in order to ensure greater consistency in implementation of the NASA Export Control Program across the Agency. We will include provisions for a dynamic, risk-based assessment of key technologies in the Export Control Program Manual that is currently in development.

QUESTION 12:

The GAO report notes that at seven centers, the Center Export Administrator was at least three organizational levels below the Center Director, despite the NASA Policy Directive that the position is to be "senior level." Three Center Export Administrators noted that this organizational placement made it difficult to maintain authority, visibility to staff, and communicate concerns to the Center Director.

- a. Where would you recommend placing the Center Export Administrator in a center's staff structure? How much contact should the CEA have with the Center Director and with center staff?

ANSWER 12:

In response to a GAO recommendation, we will revise the NASA Procedural Requirements (NPR 2190.1B) to specify the level of senior-level officials at GS-15 or above for the CEA function. The reporting structure will also be revised, so that CEAs will report directly to Center Directors or their designees in the performance of their functions. This reorganization will minimize institutional barriers between the CEAs and Center Directors allowing for more responsive management action to any identified deficiencies.

QUESTION 13:

Has there been any internal resistance regarding changing the organizational placement of the Center Export Administrators?

ANSWER 13:

NASA management is not aware of internal resistance regarding the planned changes in organizational placement of the Center Export Administrators.

QUESTION 14:

Ms. Robinson's written testimony noted that NASA lacks an efficient mechanism to resolve disputes between export control personnel and project personnel. What mechanisms could you recommend for resolving such disputes? Are there other interdisciplinary processes that could serve as a model for improving the export control and foreign national access management processes?

- a. How would you recommend encouraging scientists and engineers to consult with export control professionals regarding guidelines for projects involving

foreign nationals

ANSWER 14:

Any effective compliance program requires management commitment and an active outreach and training program. In response to a NAPA report recommendation, NASA is updating its Export Control Training Program Plan to include revised training information and position-specific training materials. Additionally, NASA has secured commitments from both the State Department and Commerce Department to provide advice and review of our enhanced training materials. Training modules for Center Export Administrators, Export Control Representatives, Program Managers, foreign national escorts, foreign national sponsors, and project personnel will be updated and deployed in NASA's online training system, SATERN. A review of compliance with training requirements also will be incorporated into the annual Export Control Program audit.

On May 8, 2014, NASA Administrator Bolden directly addressed export control officials from across the Agency about the critical role they play in safeguarding sensitive NASA technologies. That same day, he also communicated to all NASA employees the importance of the responsibility that they each have to safeguard sensitive NASA technologies by complying with all export control regulations and foreign national access management requirements. He further reminded employees that safeguarding sensitive information is a serious matter and that penalties for noncompliance can include fines and imprisonment, as well as administrative personnel actions, such as reduction-in-grade or even termination. NASA will continue to take advantage of opportunities to reaffirm with Agency employees the Administrator's message and the Agency's commitment to compliance through all levels of NASA's senior leadership.

In addition to these efforts, NASA encourages close collaboration and consultation among both scientists and engineers, and export control and security professionals regarding projects involving foreign participation during all phases of those projects. This is something that is taught in formal International Program and Project Management courses, as well as in Center-specific export control-related training sessions. Unresolved internal disputes on export control-related matters can be referred to NASA leadership where necessary, but it is anticipated that resolution and agreement without higher referral will be achieved wherever practicable, in order to ensure smooth functioning of the NASA export control program.

QUESTION 15:

There are several instances noted throughout these reports where individual NASA employees made decisions that did not value the importance of foreign national access control or ITAR restrictions. For example, the OIG report notes that Jiang's sponsor viewed Jiang's security plan, as "boilerplate" because the work Jiang was doing did not have anything to do with security. The OIG Ames report noted that on two occasions, a

senior Ames manager inappropriately shared documents with unlicensed foreign nationals that contained ITAR markings or were otherwise identified as containing ITAR-restricted information.

- a. How can NASA better educate employees, particularly when NAPA found that some NASA Centers "take a more laissez-faire approach with training either being optional or, if mandatory, provides no sanctions against those who fail to take the training?"

ANSWER 15:

Based upon the NAPA recommendations, NASA is developing a training module specifically targeted to our technical community (scientists and engineers) that will clearly communicate the threat and risk associated with information technology resources, facilities, and specific NASA assets. The Office of Protective Services Counterintelligence Division and the Insider Threat Program are collaborating on the development of this mandatory training that will help ensure consistent awareness across the Agency.

QUESTION 16:

NAPA's testimony stated that threats were inadequately conveyed to center personnel, and that training materials available from other agencies were not utilized to educate NASA staff on threats posed by insiders, hostile intelligence services, terrorism, and economic espionage.

- a. Can you recommend a strategy for better conveying these threats to center personnel?

ANSWER 16:

Based upon the NAPA recommendations, NASA is developing a training module specifically targeted to our technical community (scientists and engineers) that will clearly communicate the threat and risk associated with information technology resources, facilities, and specific NASA assets. The Office of Protective Services Counterintelligence Division and the Insider Threat Program are collaborating on the development of this mandatory training that will help ensure consistent awareness across the Agency.

QUESTION 17:

Your written testimony noted that the Administrator encouraged employees to meet with their local export control officials to learn more about NASA's Export Control Program and their responsibilities in protecting sensitive technologies.

- a. Do you know how many, if any, employees subsequently met with their local export control officials?

ANSWER 17:

CEAs have reported that nearly 500 individual inquiries from NASA employees concerning the Export Control Program have been generated as a result of the Administrator's May 8, 2014, message. Inquiries range from simple requests for additional information to requests for formal briefs to program participants. These inquiries are in addition to the CEAs' normal level of outreach to NASA programs.

QUESTION 18:

NAPA's testimony noted that tensions exist between Center Export Administrators and researchers, which can affect compliance with necessary protocols. How can NASA decrease these tensions and increase cooperation between researchers and CEAs?

ANSWER 18:

The cooperation of both CEAs and researchers is vital to the success of the NASA Export Control Program. Firm management commitment and an active outreach and training program can help to achieve this goal. Accordingly, in response to a NAPA report recommendation, NASA is updating its Export Control Training Program Plan to include revised training material and training materials specifically tailored to specific positions, such as researchers. NASA has secured commitments from both the State Department and Commerce Department to provide advice and review proposed enhancements of NASA's training materials. Training modules for Center Export Administrators, Export Control Representatives, Program Managers, foreign national escorts, foreign national sponsors, and project personnel will be updated and deployed in NASA's online training system, SATERN. A review of compliance with training requirements also will be incorporated into the annual Export Control Program audit.

As noted before, Administrator Bolden has also communicated to all NASA employees the importance of the responsibility that they each have to safeguard sensitive NASA technologies by complying with all export control regulations and foreign national access management requirements. He further reminded employees that safeguarding sensitive information is a serious matter and that penalties for noncompliance can include fines and imprisonment, as well as administrative personnel actions, such as reduction-in-grade or even termination.

In addition to these efforts, NASA encourages close collaboration and consultation among both scientists and engineers, and export control and security professionals regarding projects involving foreign participation during all phases of those projects. This is something that is taught in formal International Program and Project Management courses, as well as in Center-specific export control-related training sessions. Unresolved internal disputes on export control-related matters can be referred to NASA leadership where necessary, but it is anticipated that resolution and agreement without higher referral will be achieved wherever practicable, in order to ensure smooth functioning of

the NASA export control program.

QUESTION 19:

The NAPA team recommended that NASA use cross-functional teams to review center FNAME operations, examining both individual program compliance metrics and overall performance and outcomes. Review teams would include Headquarters program specialists and foreign national access management staff from other centers. This is in contrast to the present practice of organizational-specific compliance audits.

- a. What is your assessment of this recommendation? Do you have any additional suggestions for how to make these cross-functional reviews a success?

ANSWER 19:

On March 10, 2014, NASA established the Foreign National Access Management Program. This program will focus on improving the efficiency and effectiveness of an inherently complex process and support our mission. The purpose of this program is to address findings within the NAPA report in a systematic and coordinated approach across the Agency.

NASA currently evaluates sponsoring and requesting of foreign nationals as a component of its Integrated Security Functional Review Program. The Integrated Security Functional Review is led by the Office of Protective Services and is cross-functional in that it includes representatives from the Office of International and Interagency Relations and the Office of the Chief Information Officer. NASA is currently evaluating this program to identify areas for expansion to address specific foreign national access management processes.

QUESTION 20:

The letter to GAO appended to your testimony indicates that NASA held its yearly Export Control Program Review at Langley Research Center in May. Please summarize the issues discussed at this review. Were any additional decisions made?

ANSWER 20:

The Annual Export Control Program Review provided a forum for NASA's export control personnel to learn of recent changes in export control regulations with briefings from the Departments of Commerce, State, and Defense; to hear the findings from the NAPA, GAO and NASA OIG reviews of NASA's foreign national management and export control programs; to receive classified threat briefings by NASA Counterintelligence Special Agents and Department of Homeland Security Regional Officers; and to exchange best practices and raise compliance issues and concerns.

Also at this meeting, the HEA briefed the CEAs on the new process to document and report on actions and issues raised by CEAs. Issues and comments were documented by

support staff and merged into actions. Issues raised spanned the topics of the Foreign National Access Management Program, the marking of hardware and technical information, questions concerning NASA export control policies, and the resources and organizational issues surrounding CEA functions. The HEA assigned due dates for each action and will report on progress during quarterly videoconferences with the NASA Export Control Program community. Participants will have the opportunity to raise additional concerns or issues during the videoconferences. As appropriate, these issues will also be adopted for action, and reviewed at future videoconferences. This approach will establish a continuous process for CEAs and other NASA Export Control Program professionals to raise issues and understand the progress on their resolution. This process for continuous improvement will be documented in the Export Control Program Manual that is currently in development.

The Annual Export Control Program Review is not a decision-making forum, but a means of keeping export control personnel informed and trained, and for collecting issues and concerns for future actions and program improvement.

QUESTION 21:

Your written testimony noted that penalties for noncompliance with export control regulations and foreign national access management requirements can include fines, imprisonment, or administrative personnel actions. However, several of the relevant reports noted that reprimands for export control violations are extremely rare.

- a. How often have NASA personnel or contractors been reprimanded for export control or ITAR violations in the past four years?

ANSWER 21:

NASA is committed to reviewing recommendations by independent evaluators such as the General Accountability Office (GAO) and to having those evaluations inform changes in the Agency's existing processes in order to better safeguard access to NASA facilities by foreign nationals and to improve the protection of sensitive technologies. The referenced GAO report as well as other recent independent investigations into export control and foreign nationals access management processes have the Administrator's personal attention and he has ordered a series of changes, to include increased employee accountability, revised Agency policies and procedures and improved employee training so as to prevent incidents like this from happening again.

The protection of sensitive technologies is the personal responsibility of all NASA employees and a responsibility that every NASA manager, up to and including the Administrator himself, takes very seriously. Therefore, in May 2014, Administrator Bolden directly addressed those officials from across the Agency who manage the implementation of NASA's Export Control Program about the critical role they play in safeguarding sensitive NASA technologies. He also issued a communication to all NASA employees reminding them of their responsibility to comply with all export control regulations and foreign national access management requirements. His message

stressed that safeguarding sensitive information is a serious matter and that penalties for noncompliance can include fines and imprisonment, as well as administrative personnel actions, such as reduction-in-grade or even termination.

It is important to note that the recent independent reviews conducted by the GAO, the National Academy of Public Administration (NAPA) and NASA's own Inspector General's Office did not identify any instances when NASA employees maliciously bypassed export-control restrictions, thereby violating Federal laws, nor did they document any occurrences of NASA employees purposefully sharing sensitive information with foreign nationals. Instead, the independent reviews identified instances of employee carelessness and poor judgment with respect to export-control and foreign national access procedures at NASA Centers, which led to policy and procedural violations. These findings resulted mostly from employee confusion regarding individual roles and responsibilities in the export control and foreign national access management process. Given this confusion, Administrator Bolden directed Associate Administrator Lightfoot to assess these independent review findings and to recommend any potential corrective action in terms of Agency policies and procedures with regard to these findings. Additionally, instances of alleged violation of Agency policies by specific NASA employees have been and will be handled administratively using established disciplinary processes.

Responses by Ms. Belva Martin

**Questions For the Record and GAO Responses
July 2014**

**Questions submitted by Rep. Steven Palazzo, Chairman, Subcommittee on Space and
Rep. Paul Broun, Chairman, Subcommittee on Oversight**

1. Scientific and Technical Information that is intended to be released outside of NASA is required to be reviewed in order to ensure it does not include sensitive information. The GAO report stated that "Based on our review of NASA's most recent STI compliance audits, most centers continue to release STI that has not been reviewed for export control purposes." GAO also found that 20 percent of released information was not reviewed. GAO went on to state "We did not assess STI documents that were not reviewed or information that was posted on NASA websites without export control review to determine if their release violated export controls, but without the completion of these reviews, NASA is at increased risk of inadvertently releasing controlled technologies."
 - a. What is NASA doing to ensure that it is not releasing sensitive information?
 - b. In some instances GAO noted that this was a result of " ... deliberate action by authors to avoid export control review of papers prior to release." It appears as though NASA is both negligent in failing to review the release of information and in some instances employees are actively working to avoid reviews. What is NASA doing to reprimand those that attempt to violate federal regulations? How many individuals has NASA reprimanded for this behavior?

a. In GAO's report (*Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the Risk of Unauthorized Access to Its Technologies*, GAO-14-315), NASA has procedures in place to help prevent the release of sensitive information and also has begun conducting integrated reviews of export controls and security. However, until NASA addresses the identified deficiencies in its oversight tools and identifies the most sensitive technologies to protect, its ability to effectively protect sensitive information is limited.

b. GAO did not assess NASA's actions for those individuals that violated federal regulations, so we are not in a position to comment on NASA efforts to reprimand those individuals.
2. GAO's written testimony stated that NASA's procedural requirements for Scientific and Technical Information requires that all STI intended for release outside NASA or presented at internal meetings where foreign persons may be present must undergo technical, legal, and export control reviews?
 - a. How does this currently take place? How much time does it take?
 - b. Do NASA project personnel have concerns with this process?
 - c. What recommendations would you suggest to accommodate NASA project personnel's concerns while still accomplishing the needed reviews?

a. NASA's procedural requirement for STI requires that all STI intended for release outside of NASA or presented at internal meetings where foreign persons may be present undergo technical, legal, and export control reviews, among others, to ensure that information is not unintentionally released through publication. The CEA or a designated representative is required to sign a form showing confirmation of their export control review electronically or on a hard copy document STI form. NASA's Office of the Chief Information Officer is responsible for implementing the STI requirements and does so through its program office at Langley Research

Center. This office is required to collect and maintain STI data to measure performance trends to determine the value of the STI Program. The STI program also conducts compliance audits annually at all centers (excluding JPL) to determine how well centers are complying with the STI process and whether all STI released went through the process.

b.c. As GAO noted in its report GAO-14-315, NASA's STI program office is working with STI managers at each center to emphasize the existing requirement for export control review of STI before it is released outside of NASA. In addition, we reported Center Export Administrators' concerns that they lack resources to conduct their work in a timely manner, which in some cases, creates a backlog of work and we recommended that NASA assess CEA workload and other factors to determine appropriate resources needed to support the CEA function at each center. For example, we were told of review backlogs at one center that led to additional staff added to the export control function at this center. However, until NASA addresses identified deficiencies in oversight tools and identifies the most sensitive technologies to protect, its ability to take a risk-based approach and effectively target resources is limited.

3. **The Committee is aware of allegations of "venue-shopping" in order to gain permission to release sensitive information. When a request to release information is turned down by one reviewing official, the requestor will simply ask someone else either in the center or at headquarters until they get approval.**

- a. **How much contact do Center Export Administrators have with one another? What opportunities do you see for improving NASA's security through collaborative work by Center Export Administrators at centers and headquarters to prevent "venue-shopping?"**

a. As noted in GAO-14-315, NASA headquarters export control officials hold annual export control program reviews with the Center Export Administrators to discuss export control changes and CEA concerns and recommendations for the program. Since the topics for these meetings vary, NASA could choose to have "venue-shopping" as a discussion topic to solicit views of the CEAs.

4. **One of the problems illustrated in the NASA Office of Inspector General report on Bo Jiang is that having too many layers of bureaucracy involved in foreign national access management may negatively affect enforcement of restrictions. What specific recommendations do you have for standardizing and streamlining the process of screening foreign national visitors across centers?**

As noted in GAO-14-315, we recommend that NASA develop plans, with specific time frames, to monitor corrective actions related to management of foreign national access to NASA facilities and assess their effectiveness. NASA concurred with this recommendation and indicated that it plans to take action to increase the effectiveness of its existing procedures and implement improvements. Collectively, improvements in each of the areas we noted as deficiencies can help NASA strike an effective balance between protecting the sensitive export-controlled technologies and information it creates and uses and supporting international partners and disseminating important scientific information as broadly as possible.

5. **The OIG report on Bo Jiang describes a list of 32 provisos that can be attached to a foreign national's request for access to a center. The report noted that many employees, even in the Export Control office, did not understand some of the provisos but applied them nonetheless. For example, Jiang's plan included the**

proviso "The visit is approved based on no cost to NASA; payment of stipends/expenses against a NASA grant/contract/agreement is not authorized," despite the fact that Jiang was to be paid as a NASA contractor.

- a. Would the system be more effective with fewer provisos that were more applied?
- b. Are there any provisos that you think should be discarded?
- c. Are there any provisos that you think should be added?

a. b. c. GAO did not assess the effectiveness of NASA's provisos for foreign nationals. NASA may review these provisos as part of its comprehensive review of the program.

6. Are there any security guidelines that NASA should consider eliminating? Are there any security guidelines that NASA should consider adding?

GAO examined NASA's foreign national access control plans and procedures, and found that plans are only required when working with countries that are not members of NATO or are not major non-NATO allies. According to one CEA, control plans are not written unless the export control office pushes programs to write them. Another CEA explained that programs do not review control plans often enough to keep up with changing access needs for foreign nationals. In March 2013, CEAs requested that NASA headquarters clarify the control plan requirements and update the export control NPR to make control plans mandatory for all programs and projects with foreign national participation, regardless of country of origin. NASA formed a working group to revise the format and content of control plans, which is in the formative stages.

7. NASA uses the Identity Management and Account Exchange (IdMAX) system to process individuals requesting access to NASA facilities. How does IdMAX compare to systems used by other agencies, and to systems used by NASA in the past? Should NASA consider switching to a different system?

GAO did not assess NASA's IdMAX system. We expect that NASA will review this system as part of its comprehensive review of the foreign national access program.

8. The GAO report noted that "the resources assigned to export controls at centers did not always appear to be commensurate with the export control workload." How would you recommend that NASA go about realigning staffing levels with workload?

- a. Should NASA hire additional export control personnel, or involve more existing personnel in export control and foreign national access management?

In our report (GAO-14-315), we noted that Center Export Administrators (CEAs) have raised concerns that they lack resources to conduct their work in a timely manner, which in some cases, creates a backlog of work, and we recommended that NASA assess CEA workload and other factors to determine appropriate resources needed to support the CEA function at each center. NASA concurred with our recommendation and indicated that it had already begun to assess the need for additional resources to support the CEA function. However, until NASA addresses the deficiencies raised in oversight tools and identifies the most sensitive technologies to protect, its ability to take a risk-based approach and effectively target resources is limited.

9. The GAO report noted that at seven centers, the Center Export Administrators was at least three organizational levels below the Center Director, despite the NASA Policy

Directive that the position is to be "senior level. Three Center Export Administrators noted that this organizational placement made it difficult to maintain authority, visibility to staff, and communicate concerns to the Center Director.

- a. Where would you recommend placing the Center Export Administrator in a Center's staff structure? How much contact should the CEA have with the Center Director and with center staff?**

a. In our report, we noted that the placement of the CEA position and level of authority varies across centers and that the CEA position should allow access to the Center Director and provide authority to enforce export controls. NASA concurred with our recommendation to establish guidance defining the appropriate level and organizational placement of the CEA function. One of the CEAs stated that his placement as Special Assistant to the Center Director creates a supportive environment to incorporate export controls into the project management processes and to require and provide export control training for the majority of center staff.

- 10. Ms. Robinson's written testimony noted that NASA lacks an efficient mechanism to resolve disputes between export control personnel and project personnel. What mechanisms could you recommend for resolving such disputes? Are there other interdisciplinary processes that could serve as a model for improving the export control and foreign national access management processes?**

- a. How would you recommend encouraging scientists and engineers to consult with export control professionals regarding guidelines for projects involving foreign nationals?**

a. As noted in GAO-14-315, we recommended that NASA develop plans with specific time frames to monitor corrective actions related to management of foreign national access to NASA facilities and assess their effectiveness. NASA concurred with this recommendation and indicated that it plans to take action to increase the effectiveness of its existing procedures and implement improvements. It will be important for all NASA personnel to understand the importance of striking the appropriate balance between protecting sensitive export-controlled technologies and sharing information with international partners and others as broadly as possible.

- 11. There are several instances noted throughout these reports where individual NASA employees made decisions that did not value the importance of foreign national access control or ITAR restrictions. For example, the OIG report notes that Jiang's sponsor viewed Jiang's security plan as "boilerplate" because the work Jiang was doing did not have anything to do with security. In the OIG Ames report, it is noted that on two occasions, a senior Ames manager inappropriately shared documents with unlicensed foreign nationals that contained ITAR markings or were otherwise identified as containing ITAR-restricted information.**

- a. How can NASA better educate employees, particularly when NAPA found that some NASA centers "take a more laissez-faire approach with training either being optional or, if mandatory, provides no sanctions against those who fail to take the training?"**

a. Subsequent to our report, the NASA Administrator issued an email to all employees reiterating the importance of the export control program and announcing plans to expand the online and in-person export control training. This is an important step as it sets a tone from the top and could help ensure the centers apply consistent approaches. However, it will be

important for NASA to be vigilant in assessing action taken to help ensure effective implantation and to avoid a relapse into the former practices.

12. NAPA's testimony stated that threats were inadequately conveyed to center personnel, and that training materials available from other agencies were not utilized to educate NASA staff on threats posed by insiders, hostile intelligence services, terrorism, and economic espionage.

a. Can you recommend a strategy for better conveying these threats to center personnel?

a. NASA has procedures in place to help prevent the release of sensitive information and also has begun conducting integrated reviews of export controls and security, to include counterintelligence. GAO recommended that NASA implement a risk-based approach to the export control program by using existing information sources, such as counterintelligence assessments, to identify targeted technologies and then direct that the types and location of those export-controlled technologies are identified and managed by CEAs within each center.

13. How do other agencies manage their foreign national employees' and visitors' access to sensitive information? Is there a "gold standard" or model in place for NASA to work toward?

GAO did not assess other agencies management of foreign national employees or visitor access to sensitive information during our review of NASA export controls.

14. NAPA's testimony noted that tensions exist between Center Export Administrators and researchers, which can affect compliance with necessary protocols. How can NASA decrease these tensions and increase cooperation between researchers and CEAs?

As noted in GAO-14-315, we recommended that NASA develop plans with specific time frames to monitor corrective actions related to management of foreign national access to NASA facilities and assess their effectiveness. NASA concurred with this recommendation and indicated that it plans to take action to increase the effectiveness of its existing procedures and implement improvements. Setting the tone from the top about the importance of the export control program, as well as implementing improvements in each of the areas we noted as having deficiencies, and can help NASA strike an effective balance between protecting the sensitive export-controlled technologies and information it creates and uses and supporting international partners and disseminating important scientific information as broadly as possible.

15. The NAPA team recommended that NASA use cross-functional teams to review center FNAM operations, examining both individual program compliance metrics and overall performance and outcomes. Review teams would include Headquarters program specialists and foreign national access management staff from other centers. This is in contrast to the present practice of organizational-specific compliance audits.

a. What is your assessment of this recommendation? Do you have any additional suggestions for how to make these cross-functional reviews a success?

a. NASA has procedures in place to help prevent the release of sensitive information and also has begun conducting integrated reviews of export controls and security, to include

counterintelligence. NASA concurred with GAO's recommendation to implement a risk-based approach to the export control program by using existing information sources, such as counterintelligence assessments, to identify targeted technologies and then direct that the types and location of those export-controlled technologies are identified and managed by CEAs within each center.

16. The NAPA report recommended the creation of an Asset Protection Oversight Board.
a. Do you think creating the Asset Protection Oversight Board is a fruitful course of action?

a. NASA lacks a comprehensive inventory of the types and location of export-controlled technologies at the centers, limiting their ability to identify internal and external risks to export control compliance. Three centers began recent efforts to identify export-controlled technologies at their centers. To implement a risk-based approach, we recommended NASA build off of existing information sources, such as assessments by NASA's counterintelligence office, to identify targeted technologies. In its response, NASA highlighted plans to implement a risk-based approach that would include CEAs, program managers, and counterintelligence officials. Determining the best way to implement a risk-based approach will likely involve several courses of action. An Asset Protection Board could help NASA to implement a more risk-based approach.

Questions For the Record From RM Donna F. Edwards
"NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information"

1. How can Congress ensure that NASA deals with your recommendations in an effective and efficient manner? What are some options for evaluating NASA's implementation of these recommendations?

It will be important for NASA to be vigilant in assessing action taken to help ensure effective implementation and to avoid a relapse into the former practices. Congress could consider requiring NASA to report to Congress in one year from the date of the hearing (June 2014), on the steps it has taken and actions implemented in response to the recommendations in GAO's report. GAO will also follow-up with NASA annually to assess progress in implementing the recommendations.

2. You testified on the importance of NASA implementing a risk management process to identify and prioritize vulnerable assets, among other things. What would an effective risk management process look like? Are there examples from other Federal agencies that NASA could use in developing such a process?

NASA highlighted plans to implement a risk-based approach that would include CEAs, program managers, and counterintelligence officials. Also, as we reported in GAO-14-315, determining the best way to implement a risk-based approach will likely involve several courses of action. State and Commerce elements of an effective compliance program state the importance of identification of controlled items, as well as a continuous risk assessment of the program. For example, Commerce's Compliance Guidelines suggest nine elements of an effective compliance program and that a key step in addressing risk is to assess areas of vulnerability, including a technical assessment of export-controlled items.

3. **Ms. Robinson's statement appears to be supportive of making use of Export Control Representatives, a model you found at JPL that has engineers and scientists work with JPL's export control staff. Do you agree that such a model could help address the lack of early interaction between project managers and export control staff at other Centers?**

As stated in GAO-14-315, NASA procedures allow CEAs to establish a network of Export Control Representatives to assist with export determinations and reviews and coordinate export control issues with the CEA. The Export Control Representative is to maintain a working knowledge of the export control laws and regulations. Six of the 10 centers had established networks of Export Control Representatives, ranging from the use of 1 at one center to 600 of these representatives at another center. We did not assess the reasons for the wide variability in use of Export Control Representatives. If NASA is considering using these representatives, it will be important to obtain input from the CEAs that do or do not use them as well as developing uniform requirements, including training.

Responses by Ms. Gail A. Robinson

**HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON SPACE
SUBCOMMITTEE ON OVERSIGHT**

“NASA Security: Assessing the Agency’s Efforts to Protect Sensitive Information”

Questions for the Record, Gail Robinson, Deputy Inspector General, National Aeronautics and
Space Administration Office of Inspector General

**Questions submitted by Rep. Steven Palazzo, Chairman, Subcommittee on Space and
Rep. Paul Broun, Chairman, Subcommittee on Oversight**

1. Ms. Martin’s written testimony stated that NASA’s procedural requirements for Scientific and Technical Information requires that all STI intended for release outside NASA or presented at internal meetings where foreign persons may be present must undergo technical, legal, and export control reviews.
 - a. How does this currently take place? How much time does it take?
 - b. Do NASA project personnel have concerns with this process?
 - c. What recommendations would you suggest to accommodate NASA project personnel’s concerns while still accomplishing the needed reviews?

The Office of Inspector General (OIG) does not have data on how long this process takes generally. However, as we noted in our Ames report in some instances the review can take many months. Similarly, the National Academy of Public Administration (NAPA) reported that Center Export Control Administrators (CEA) “spend a great deal of time reviewing research papers” and “often find themselves at odds” with the authors of these papers. As I suggested in my testimony, working toward a model that encourages Agency scientists and engineers to consult with export professionals when projects involving foreign nationals are initiated and developing a mechanism for resolving disputes in a timely manner could help NASA improve the review process.

2. The OIG’s reports regarding Langley and Ames point to a great deal of confusion regarding the roles, responsibilities, and requirements for contractors - particularly in instances where NASA Centers house non-governmental “institutes” like the National Institute of Aerospace (NIA) at Langley. The IG’s report on Jiang stated “NIA appeared to lack sufficient procedures to ensure that appropriate officials in its organization were informed of the restrictions NASA placed on Jiang’s access to the Center [Langley].”
 - a. How can NASA and contractors prevent foreign nationals from slipping through the cracks and obtaining inappropriate access to NASA IT resources and facilities?

Over the past year, the OIG, Government Accountability Office (GAO), and NAPA each made a series of recommendations to improve NASA’s foreign national access program. We believe timely and effective implementation of these recommendations will help NASA ensure that foreign nationals do not obtain inappropriate access to NASA IT resources and facilities.

3. One of the problems illustrated in the NASA Office of Inspector General report on Bo Jiang is that having too many layers of bureaucracy involved in foreign national access management may negatively affect enforcement of restrictions. What specific recommendations do you have for standardizing and streamlining the process of screening foreign national visitors across Centers?

With regard to streamlining, as we recommended in the Jiang report NASA needs to examine and realign the roles and responsibilities of personnel involved in its foreign national access process and ensure the appropriate offices are represented and responsibilities appropriately assigned. With regard to standardization, we agree with NAPA's recommendations to create a programmatic office located at NASA Headquarters to centralize the Agency's overall foreign national access process and that NASA significantly reduce the flexibility Centers have to change aspects of the Agency's overall process and systems regarding foreign national access.

4. The OIG report on Bo Jiang describes a list of 32 provisos that can be attached to a foreign National's request for access to a center. The report noted that many employees, even in the Export Control office, did not understand some of the provisos but applied them nonetheless. For example, Jiang's plan included the proviso "The visit is approved based on no cost to NASA; payment of stipends/expenses against a NASA grant/contract/agreement is not authorized," despite the fact that Jiang was to be paid as a NASA contractor.
 - a. Would the system be more effective with fewer provisos that were more strictly applied?
 - b. Are there any provisos that you think should be discarded?
 - c. Are there any provisos that you think should be added?

As discussed in our Jiang report, the problem appeared to be less with the number or nature of the provisos and more with staff applying them to circumstances to which they did not fit. In addition, as we noted in the report the Export Control Office removed two provisos – one that referred to a visa requirement and one providing that no NASA funds be expended – on the grounds that these issues should be determined by NASA security and procurement personnel rather than Export Control officials. Another problem, as noted in our report, was that the civil servants directly responsible for overseeing Jiang were never informed of the provisos which, in turn, prevented them from questioning whether the provisos were appropriate or necessary.

5. Are there any security guidelines that NASA should consider eliminating? Are there any security guidelines that NASA should consider adding?

In our Jiang report, we recommended NASA revise its Security Technology Transfer Control Plans to include a description of Agency policy regarding taking information technology equipment out of the United States.

6. The OIG report on Ames stated that there was “significant disagreement between scientists and engineers at Ames and export control personnel at the Center and NASA headquarters as to whether the work the foreign nationals were performing ... involved ITAR controlled technology.” Similarly, the GAO found that “NASA lacks a comprehensive inventory of export-controlled technologies and is not fully utilizing oversight tools.” It appears as though NASA doesn’t even know what information it needs to protect.
 - a. Who is responsible at each center and at headquarters for cataloging ITAR and export controlled information?

NASA Procedural Requirements (NPR) 2190 sets forth roles and responsibilities for NASA’s export control program. Although the NPR provides that NASA program managers are to identify, in consultation with CEAs, export-controlled data and technologies relating to their projects, it does not assign any individual or office the specific responsibility of “cataloging” ITAR and export-controlled information. As discussed in my testimony, we encountered a situation in a recently completed investigation in which a CEA was not aware that an off-site lab under his responsibility contained export-controlled equipment and data. A first step would be to ensure that CEAs are familiar with all export-controlled equipment and data at their Centers and related facilities.

7. NASA uses the Identity Management and Account Exchange (IdMAX) system to process individuals requesting access to NASA facilities. How does IdMAX compare to systems used by other agencies, and to systems used by NASA in the past? Should NASA consider switching to a different system?

The OIG does not have information about former NASA systems or systems used by other agencies. NASA indicated in response to NAPA’s recommendations that it will conduct a review of IdMAX as part of establishing a Foreign National Access Management Program.

8. The GAO report notes that at seven centers, the Center Export Administrator was at least three organizational levels below the Center Director, despite the NASA Policy Directive that the position is to be “senior level.” Three Center Export Administrators noted that this organizational placement made it difficult to maintain authority, visibility to staff, and communicate concerns to the Center Director.
 - a. Where would you recommend placing the Center Export Administrator in a center’s staff structure? How much contact should the CEA have with the Center Director and with center staff?

As discussed in my testimony, we believe it important for CEA’s to work closely with project staff to ensure appropriate handling of export-controlled information. With regard to the Center Director, we believe a clear message that the CEA has the support and backing of the Center’s senior leadership is important.

9. Your written testimony notes that NASA lacks an efficient mechanism to resolve disputes between export control personnel and project personnel. What mechanisms could you recommend for resolving such disputes? Are there other interdisciplinary processes that could serve as a model for improving the export control and foreign national access management processes?

- a. How would you recommend encouraging scientists and engineers to consult with export control professionals regarding guidelines for projects involving foreign nationals?

As I noted in my testimony, NASA policy allows for appointment of project personnel as Export Control Representatives (ECR) to coordinate export control issues with CEAs and assist them with reviews and determinations. We believe a strong network of ECRs at all Centers could help bridge the gap between project personnel and export control professionals.

10. There are several instances noted throughout these reports where individual NASA employees made decisions that did not value the importance of foreign national access control or ITAR restrictions. For example, the OIG report notes that Jiang's sponsor viewed Jiang's security plan as "boilerplate" because the work Jiang was doing did not have anything to do with security. The OIG Ames report noted that on two occasions, a senior Ames manager inappropriately shared documents with unlicensed foreign nationals that contained ITAR markings or were otherwise identified as containing ITAR-restricted information.

- a. How can NASA better educate employees, particularly when NAPA found that some NASA centers "take a more laissez-faire approach with training either being optional or, if mandatory, no sanctions against those who fail to take the training?"

As NAPA recommended, NASA could standardize and enhance its Counter Intelligence (CI) training and education programs to ensure that employees understand potential threats, which in turn could help ensure a better appreciation of the importance of complying with export control restrictions. NASA concurred with NAPA's recommendation.

11. NAPA's testimony stated that threats were inadequately conveyed to center personnel, and that training materials available from other agencies were not utilized to educate NASA staff on threats posed by insiders, hostile intelligence services, terrorism, and economic espionage. Can you recommend a strategy for better conveying these threats to center personnel?

As noted above, NASA is developing a CI training module that responsible personnel will be required to complete on an annual basis. Implementation of this module should improve employees' understanding and appreciation of such threats.

12. NAPA's testimony noted that tensions exist between Center Export Administrators and researchers, which can affect compliance with necessary protocols. How can NASA decrease these tensions and increase cooperation between researchers and CEAs?

As noted in response to question 9, effective use of ECRs could help address this issue.

13. The NAPA team recommended that NASA use cross-functional teams to review center FNAM operations, examining both individual program compliance metrics and overall performance and outcomes. Review teams would include Headquarters program specialists and foreign national access management staff from other Centers. This is in contrast to the present practice of organizational-specific compliance audits.

- a. What is your assessment of this recommendation? Do you have any additional suggestions for how to make these cross-functional reviews a success?

We sometimes use cross-functional teams to conduct OIG reviews and believe they can be helpful if they include personnel with the skill mix that matches the assigned task.

14. The NAPA report recommended the creation of an Asset Protection Oversight Board.

- a. Do you think creating the Asset Protection Oversight Board is a fruitful course of action?

We believe an oversight board could be helpful and agree with NASA's intention to explore utilizing an existing council to accomplish this function.

Questions for the Record
From RM Donna F. Edwards
“NASA Security: Assessing the Agency’s Efforts to Protect Sensitive Information”

1. How can Congress ensure that NASA deals with your recommendations in an effective and efficient manner? What are some options for evaluating NASA’s implementation of these recommendations?

Congress can ensure NASA addresses recommendations made by the OIG, GAO, and NAPA by requesting periodic updates and briefings from the Agency. As with all recommendations we make to NASA, the OIG will also monitor Agency compliance and may open a formal follow-up review at a later date.

2. How important is it for NASA to develop a risk management process that would allow the agency to identify and prioritize vulnerable assets, assess protective strategies, allocate resources commensurate with the risk, and evaluate the overall asset protection efforts? What, in your view, would an effective risk management process look like? Are there examples from other Federal agencies you are aware of that NASA could use in developing such a process?

As the NAPA report recognized, NASA needs to take a “comprehensive approach to risk management, employing the best practices available.” Risk management is an inherent part of establishing effective foreign national access and export control programs. NASA has significant experience with risk management in other parts of its operations to draw from in improving its asset protection efforts. We support NAPA’s recommendation that NASA establish a “mechanism for comprehensive, Center-specific assessments” and should compile “threat/risk assessments.” As NAPA noted, “This would permit HQ and Center executives to identify and prioritize vulnerable assets, assess protective strategies, allocate resources commensurate with the risk, and evaluate the overall asset protection efforts.” Failing to take these steps could result in expending resources where they are not necessary and result in a less robust approach to the problem.

3. Your statement appears to be supportive of making use of the model GAO found at JPL that has engineers and scientists work with JPL’s export control staff as export control representatives. How would this model provide a mechanism for dispute resolution, as you suggested in your prepared statement?

Because ECRs are drawn from the pool of NASA scientific and technical professionals and perform their ECR role as an additional duty, they may be in a better position to “bridge the gap” between project personnel and CEAs based on their relationships and understanding of the issues facing project personnel.

4. Are the reasons advanced by NASA personnel for the inconsistent application of and compliance with established policies regarding the automated IdMax tool indicative of insufficient awareness of risks and the absence of consequences for noncompliance? Is better training the answer?

As discussed in our Jiang report, we believe some of the mistakes employees made relating to Jiang's access were due to a misunderstanding about the meaning and effect of the provisos used by the Headquarters Export Control Office such as a Headquarters' official describing the provisos as "advisory" and a Center official describing them as "boilerplate." We also noted that much of the confusion about Jiang's access occurred either because not all the individuals in the process had access to all the relevant information or because individuals failed to exercise sufficient due diligence in completing their duties. The former issue requires retooling of processes and procedures, while additional training and sound performance management could help address the latter issue.

Responses by Mr. Douglas Webster



RESPONSES TO QUESTIONS FOR THE RECORD

Doug Webster
National Academy of Public Administration

*Questions submitted by Rep. Steven Palazzo, Chairman, Subcommittee on Space and
 Rep. Paul Broun, Chairman, Subcommittee on Oversight*

- 1) **Ms. Martin's written testimony stated that NASA's procedural requirements for Scientific and Technical Information requires that all STI intended for release outside NASA presented at internal meetings where foreign persons may be present must undergo technical, legal, and export control reviews.**
- How does this currently take place? How much time does it take?**
 - Do NASA project personnel have concerns with this process?**
 - What recommendations would you suggest to accommodate NASA project personnel's concerns while still accomplishing the needed reviews?**

1. **a RESPONSE**

Export Control policy at NASA is established by the Export Control and Interagency Liaison Division within the Office of International and Interagency Relations at NASA Headquarters. NASA's written policies provide the underlying guidance for the export control program. However, there is no manual or written set of guidelines that spell out the standardized rules for the implementation of the program throughout NASA. NASA Center directors have line authority over the export control programs within their individual Centers and have broad discretion in how these individual programs are managed. Center Export Administrators (CEAs) report to the Center director through each Center's Office of Protective Services. CEAs are responsible for reviewing sensitive information prior to release to ensure compliance with Export Control requirements.

The amount of time it takes for such reviews varies widely among NASA centers. Project staff frustration with review delays in some centers was very high while in others, the time it takes to conduct export control reviews was seen as reasonable. CEAs were also frustrated by the submission of "last minute" requests for EC reviews that project staff sometimes submit. Both staffs are sometimes in disagreement about what information needs to be export controlled. The Panel found that NASA's Export Control program needs a more standardized and systematic approach to its export compliance objectives, as well as better audit and review mechanisms.

NASA senior leaders also need to more strongly endorse the critical importance of such controls. NASA's Center Export Administrators (CEAs) are chosen by Center directors with little input from the Headquarters export control staff. CEAs are often selected by Center senior level managers who may have very little, or no, export control expertise. In some cases, based on the need for Centers to maintain a lean administrative footprint, the export control program responsibility of a CEA could be treated as an additional or ancillary duty, thereby raising the risk for inadvertent or accidental disclosures of sensitive information or unnecessary delays in reviewing materials.

1. b - RESPONSE

Yes. Academy staff spoke with over 150 NASA staff at 6 different facilities and held focus groups with project staff at each facility. Complaints and concerns about the process were widespread among four of the centers but significantly less in two centers. The main areas of concern were the length of the review process and the criteria for determining when information needs to be export controlled.

1. c - RESPONSE

Overall, the Panel found that NASA's Export Control program needs a more standardized and systematic approach to its export compliance objectives, as well as better audit and review mechanisms. NASA senior leaders also need to more strongly endorse the critical importance of such controls.

The Panel recommended that NASA take steps to systematize the approach to export control and emphasize its importance by:

- a) Providing a detailed export control manual that will serve as a standardized guide to Center staff
- b) Issuing a strongly-worded communication from senior management to NASA employees that affirms the Agency's commitment to export compliance.
- c) Conducting outside periodic reviews of the each Center's export control activities to assess and evaluate the procedural components, to include their effectiveness and efficiency.
- d) Requiring that a HQ endorsement be sought before any field CEA job is filled and that the HQ export control organization provide input into each field CEA annual rating to strengthen the linkage between Center CEAs and their HQ counterparts.

- 2) One of the problems illustrated in the NASA Office of Inspector General report on Bo Jiang is that having too many layers of bureaucracy involved in foreign national access management may negatively affect enforcement of restrictions. What specific recommendations do you have for standardizing and streamlining the process of screening foreign national visitors across centers?**

RESPONSE

The Academy Panel recommended two critical steps NASA needs to take to standardize and streamline the process:

- Manage Foreign National Access Management as a Program. Currently, FNAM is not managed as a program and there is no systematic approach to FNAM at NASA; rather,

there are individual Headquarters program requirements coupled with individual NASA Center approaches. Given inadequate means for determining the overall effect of these processes, the result is a broad range of outcomes, many of which are insufficient.

- Reduce the flexibility given to Centers to interpret FNAM requirements. Too much flexibility in largely procedural processes coupled with a “stovepiped” organizational structure and overly broad and organizationally-specific directives has resulted in inconsistent and ineffective outcomes. This includes writing a comprehensive and detailed FNAM operating manual covering all functional aspects of the program as well as conducting periodic, external, programmatic reviews of field Center FNAM.

Adopting these recommendations will eliminate much of the “stove piping” and bureaucratic layers of the current process.

3) The OIG report on Bo Jiang describes a list of 32 provisos that can be attached to a foreign national’s request for access to a center. The report noted that many employees, even in the Export Control office, did not understand some of the provisos but applied them nonetheless. For example, Jiang’s plan included the proviso “The visit is approved based on no cost to NASA; payment of stipends/expenses against a NASA grant/contract/agreement is not authorized,” despite the fact that Jiang was to be paid as a NASA contractor.

- a. Would the system be more effective with fewer provisos that were more strictly applied?
- b. Are there any provisos that you think should be discarded?
- c. Are there any provisos that you think should be added?

RESPONSE

The Academy review did not consider the specific provisos that can be attached to a foreign national’s access; however, by consolidating the process under a single program, streamlining the steps that need to be taken as well and reducing the number of individuals involved in the process, as recommended by the Academy Panel, NASA can greatly reduce the chances of Bo Jiang-type events taking place.

4) NAPA’s testimony noted that too much flexibility in a procedural process, coupled with a “stovepiped” organization structure such as NASA’s, can create inconsistency and poor outcomes. Which aspects of foreign national access management and export control require flexibility in decision making? Which aspects are best conducted with a more rigid process?

RESPONSE

The Panel believes that the overwhelming majority of FNAM processes should have clear and unambiguous procedural steps established by NASA HQ that must be followed by all NASA centers. In cases where the designated process is insufficient (e.g., unanticipated last minute requests for NASA technical presentations at conferences or foreign visitor access), then some flexibility needs to be granted to centers. These types of flexibilities should be the exceptions to the rules and should be carefully monitored by both center and HQ staffs to prevent overuse of abuse of the flexibilities.

5) Are there any security guidelines that NASA should consider eliminating? Are there any security guidelines that NASA should consider adding?

RESPONSE

The Academy does not have suggestions as to specific security guidelines which NASA should consider eliminating but has been told by NASA that the Panel's recommendation to consolidate FNAM under a single program manager is being implemented and that all FNAM security guidelines are being reviewed for inclusion in a comprehensive manual that will describe all aspects of the process.

6) NASA uses the Identity Management and Account Exchange (IdMAX) system to process individuals requesting access to NASA facilities. How does IdMAX compare to systems used by other agencies, and to systems used by NASA in the past? Should NASA consider switching to a different system?

RESPONSE

The Academy review did not look at specific IT systems used by other agencies but did note that: *IdMAX business processes and workflows do not currently support all FNAM requirements. All stakeholders, including end-users, need to be represented in its business process redesign.*

Interviewees in field Centers who use the IdMAX system pointed out a number of areas in need of improvement; however, because an Identity Credential and Access Management (ICAM) modernization project is underway, and IdMAX is a sub-element of that system, NASA is only making minor modifications to the current IdMAX application.

Though making changes to business processes are not a part of this ICAM modernization project, this would be an excellent time for NASA to begin to conduct a thorough review of the entire identity management business process. The agency should implement a workflow that incorporates input from each organization that must use the application, including end-users, with an overarching goal of streamlining and improving the process.

IdMAX business processes should be enhanced to include all FNAM requirements, including an electronic Technology Transfer Control Plan (TTCP) that automatically limits access to systems and assets based on specific criteria selected. (This would significantly reduce the Chances of another Bo Jiang incident.) A review of the current business processes should be conducted by a team consisting of representatives from all NASA ICAM stake holders at both the Centers and Headquarters. Center staff from all disciplines in the identity management and credentialing process, including sponsors, hosts and escorts, should be allowed to provide input.

- 7) The GAO report notes that “the resources assigned to export controls at centers did not always appear to be commensurate with the export control workload.” NAPA noted similar concerns regard insufficient staffing for NASA’s counterintelligence and counterterrorism program. How should NASA go about assessing and realigning staffing needs in this area?

RESPONSE

The Panel believes NASA HQ needs to standardize the approach to export controls, including guidance on how to properly staff such functions. This would include the widely variant approaches centers take in the use of Export Control Representatives (ECRs). ECRs are staff from various functional areas within the Centers who conduct export control reviews. At one Center visited, ECRs are provided extensive initial export training by an outside vendor who has delivered export training for the Center for several years. The ECRs are subsequently provided with refresher training as required. The 74 ECRs that the Center utilizes actually conduct the initial reviews and approve or request modifications to technical documents. They consult with the Center Export Administrator (CEA) staff as necessary or when there are complex issues to be decided. In general, the review of materials for export control purposes runs smoothly at this Center.

In contrast, another Center the study team visited did not use ECRs at all, and their CEA seemed overwhelmed by the sheer volume of material that needed to be reviewed. An internal review found that the Center’s export control office is hampered in its ability to keep up with the production of research and collaborative initiatives by employees of the Center. The main reason cited was the fact that the Center’s export control office has too few staff in relation to the quantity of written documents that require review. Ironically, this Center, with no ECRs, has more than twice as many export control actions as the Center mentioned above with 74 ECRs.

- 8) Mrs. Robinson’s written testimony notes that NASA lacks an efficient mechanism to resolve disputes between export control personnel and project personnel. What mechanisms could you recommend for resolving such disputes? Are there other interdisciplinary processes that could serve as a model for improving the export control and foreign national access management process?
- a. How would you recommend encouraging scientists and engineers to consult with export control professionals regarding guidelines for projects involving foreign nationals?

RESPONSE

The Panel found that most of the disputes arising from export control issues arose from poor communications, misunderstandings, and in some cases, mistrust between the export control and program staffs. In centers where scientists and engineers are more involved in export control decisions by serving as Export Control Representatives (see Q. 7 response) there are relatively few such disputes and when they arise, are readily resolved. These ECRs are better trained and have closer working relationships with export control staff and as a result, have a fast and efficient process which protects sensitive information and minimizes disputes. NAPA would

propose that NASA consider making use of ECRs a standard practice across all Centers to encourage scientists and engineers to work closer with export control professionals.

- 9) There are several instances noted throughout these reports where individual NASA employees made decisions that did not value the importance of foreign national access control or ITAR restrictions. For example, the OIG report notes that Jiang's sponsor viewed Jiang's security plan as "boilerplate" because the work Jiang was doing did not have anything to do with security. In the OIG Ames report, it is noted that on two occasions, a senior AMES manager inappropriately shared documents with unlicensed foreign nationals that contained ITAR markings or were otherwise identified as containing ITAR-restricted information.
- a. How can NASA better educate employees, particularly when NAPA found that some NASA Centers "Take more laissez-faire approach with training either being optional or, if mandatory, provides no sanctions against those who fail to take the training?"

RESPONSE

The Panel found that export control training requirements are inconsistent; the training is confusing and inadequate; and the rationale for such training is often poorly understood. It recommended that NASA revise its export control training program and develop an improved and more effective, standardized training program for educating both specialized Center export control personnel as well as other NASA employees who need to understand US export regulations.

- 10) NAPA's testimony stated that threats were inadequately conveyed to center personnel, and that training materials available from other agencies were not utilized to educate NASA staff on threats posed by insiders, hostile intelligence services, terrorism, and economic espionage.
- a. Can you recommend a strategy for better conveying these threats to center personnel?

RESPONSE

At most of the Centers visited during the Academy review, Counterintelligence (CI) Awareness and Education "for all NASA employees and contractors" (as called for in NASA policy directives) does not exist. Regarding the awareness and education briefings, NASA policy states that the briefings will be delivered "as needed." This policy interpreted differently by the individual CI Special Agents (CISA). As a result, CI awareness and education in the Centers and at HQ vary greatly, and their effectiveness in reaching employees depends in large measure on the initiative and personality of the CISAs.

CISAs appear to focus their awareness briefings on upper management rather than focusing on providing information to all employees and contractors. As a result, some employees advised that they were unaware of any CI presence at their Centers. Additionally, some of the CISA's offices are in inaccessible locations for Center employees who may have questions or want to report a concern.

Some engineers and scientists in focus groups indicated that they do not fully understand the foreign national threat to NASA and that the threat information provided during training rarely had relevance to their situations. Most personnel understand the need to protect classified information but they question whether sensitive, unclassified information needs protection. Additionally, there does not appear to be a significant emphasis on CI awareness from Agency and Center hierarchies.

The Academy Panel believes that NASA needs to provide clearer examples to center personnel of the threats posed by foreign nationals with access to NASA facilities. NASA officials noted that much of the most relevant material was classified and therefore, unable to be used during general training sessions. The Panel believes that NASA could edit the classified sections out of the material and provide more meaningful training examples that would resonate with center staff.

11) How do other agencies manage their foreign national employees' and visitors' access to sensitive information? Is there a "gold standard" or model in place for NASA to work toward?

RESPONSE

While the Academy Panel did not do a broad benchmarking analysis of other agency efforts, the program managed by the Department of Energy was seen as a good yardstick for NASA to consider because DOE's procedural documents are very comprehensive and user-friendly. While there are differences in NASA's and DOE's missions, there are enough similarities to warrant assessment of possible application of DOE's procedures, training, and oversight regarding foreign visitors to NASA.

12) NAPA's testimony noted that detailed policies and procedures for asset protection have been implemented by other agencies, particularly by the Department of Energy. What lessons from implementation at DOE could be applied to NASA? How have DOE employees reacted to these policies and procedures?

RESPONSE

The Panel believes much of what DOE has done regarding asset protection are relevant to NASA and that it would be prudent for NASA to take a closer look at DOE's implementation issues and the reaction of employees. NASA officials did indicate to the Panel that they would look at DOE's efforts.

During the NASA study, the study team spoke with several DOE officials in their Counterintelligence Office about organizational issues and the policy and procedural documents pertaining to security and counterintelligence. The sole purpose of these discussions was to point NASA to another similar agency that had significantly better written guidance and direction for their employees to follow and to identify "best practices" that NASA could assess and implement if warranted. The Academy study team did not discuss the perception of DOE staff about such issues, nor did they interview any DOE employees about this matter.

13) Your written testimony noted concerns regarding competition between centers negatively impacting NASA security. You specifically cited centers with solutions being disinclined to assist competitors and centers experiencing problems being concerned about exposing weakness in their operations.

Are there specific instances where one of these two scenarios occurred? How do you recommend addressing these issues?

RESPONSE

Academy study team members were told of specific instances where competition hampered information sharing between centers. The problem can be reduced by creating a FNAM program that can not only standardize policies and procedures but can also ensure that best practices are widely shared. As the Panel noted in its report, competition between centers may enhance program and project development but can only serve as an impediment to largely administrative/procedural operations.

14) NAPA's testimony noted that tensions exist between Center Export Administrators and researchers, which can affect compliance with necessary protocols. How can NASA decrease these tensions and increase cooperation between researchers and CEAs?

RESPONSE

A certain amount of tension is probably inherent between NASA researchers and CEAs but there are examples of centers successfully managing that tension by having very effective training (which makes clear the importance of CEA reviews of export control materials) and using Export Control Representatives (ECRs) to supplement the efforts of CEAs. Improving training and standardizing it across centers and setting standards for using ECRs would, in the Panel's opinion, eliminate most of the tension.

**15) The NAPA report recommended the creation of an Asset Protection Oversight Board.
a. Please describe the intended functions of the Asset Protection Oversight Board, including the Board's structure, jurisdiction, and proposed activities?**

RESPONSE

The task of protecting NASA's assets – its facilities, personnel, technologies, and information – is a multi-dimensional responsibility involving every NASA civil servant, contractor, and organization, as well as the support and assistance of other agencies. The successful performance of this task is dependent on completion of a number of interrelated functions – identification of assets requiring protection, accurate intelligence regarding threats, design and implementation of protective strategies, education and awareness of NASA personnel, and continuous evaluation to ensure threats are countered commensurate with their importance. This requires a comprehensive approach to risk management, employing the best practices available.

NASA needs to reconsider how it assesses and protects its information and security assets in the field. While this review has focused on FNAM, the Panel believes that a broader approach to asset protection and oversight is needed. NASA facilities, personnel, technologies, and information are highly regarded and of great interest to the world. That interest extends to some countries, governments, organizations, and individuals whose intent is to compromise those

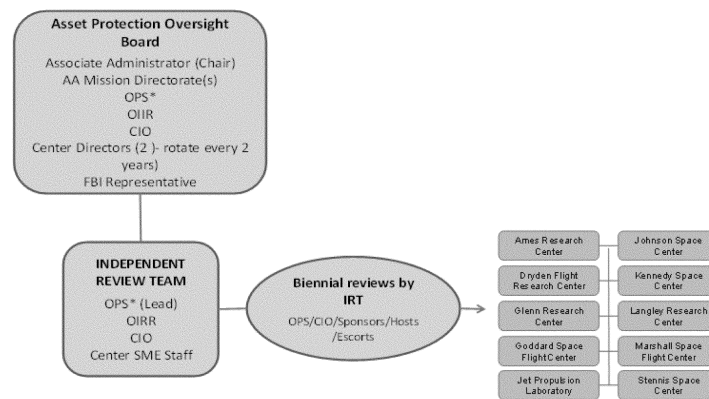
facilities, co-opt the personnel, and steal those technologies and information. While NASA currently conducts annual threat assessments at every Center by the Protective Services office, the CISAs, and the CIO, those assessments address only the areas of responsibility of those individual offices. They are not comprehensive, Center-specific assessments that consider all the elements necessary to fully protect NASA's assets.

By establishing a mechanism for comprehensive, Center-specific assessments NASA could compile threat assessments from security, CI/CT, and the CISOs into comprehensive Center and agency threat/risk assessments. This would permit HQ and Center executives to identify and prioritize vulnerable assets, assess protective strategies, allocate resources commensurate with the risk, establish and monitor controls consistent with OMB Circular A-123, and evaluate the overall asset protection efforts.

With the above considerations in mind, the Panel recommended that NASA create an Asset Protection Oversight Board to oversee the safety and security of NASA assets in the field. The overall goal of the Board is to protect all of NASA's valuable International Traffic in Arms Regulation (ITAR) and Export Administration Regulations (EAR) technical data and proprietary information, not simply the data potentially exposed to foreign nationals and to also compile threat assessments from security, CI/CT, and the CISOs into comprehensive Center and agency threat/risk assessments. The Panel also recommended that NASA create an Independent Review Team (IRT), led by the Office of Protective Services, and including membership from OIIR and CIO and field Center representatives, to biennially review all field Centers to assess and evaluate the procedural components comprising the asset protection program to also include effectiveness and efficiency. The team should operate under the guidance of the Asset Protection Oversight Board.

These assessments could be incorporated into NASA's risk management process. Specific goals and objectives for the board are listed in the "Asset Protection" narrative in Chapter 3. The Board should be supported by the HQ OPS. The structure recommended by the Panel is shown in Figure 1 below. NASA officials have indicated to the Academy that while they support the overall function of the proposed Board, they believe it should be incorporated into existing NASA's organizational board structure.

Figure 1. Asset Protection Oversight Board



Questions for the Record
From Ranking Member Donna F. Edwards
“NASA Security: Addressing the Agency’s Efforts to Protect Sensitive Information”

- 1) How can Congress ensure that NASA deals with your recommendations in an effective and efficient manner? What are some options for evaluating NASA’s implementation of these recommendations?**

RESPONSE

NASA has agreed to provide quarterly updates on their progress in implementing the Panel’s recommendations. This would provide a good baseline for ensuring that an effective and efficient process is created. A follow-up review by an external authority that includes visits to NASA HQ and field centers would provide the most comprehensive evaluation. We would also recommend that NASA consider more formally incorporating FNAM processes, controls, and risks into the OMB Circular A-123 reporting process from Centers to NASA Headquarters. As stated in the written testimony, the Academy would welcome the opportunity to conduct such a review.

- 2) In your prepared statement, you note that your panel found NASA Procedural Requirements and NASA Policy Directives regarding foreign national access to be “comprehensive, well-written, and easily accessible through NASA’s online library.” Yet, in the same paragraph, you indicate that in some cases “Centers have developed and published their own procedural requirements that were found to be more practical and user-friendly.”**

RESPONSE

- a) Is there an inconsistency between those two findings?**

NASA directives are well done, but do not provide sufficient detail to ensure that desired outcomes are achieved—that is, they do not go far enough. Overbroad directives coupled with highly independent field centers which interpret the process steps in significantly different ways leads to some of the deficiencies noted in the Academy study.

- b) Did NAPA recommend a way to make directives more practical and user friendly?**

The Academy recommendations on rewriting the directives focused on two fundamental principles: first, ensure that the various elements of the FNAM process are approached holistically, that is, each of the program staffs that author their individual sections should be working on a collaborative manual that documents the entire process; and second, field users need to be involved in the rewrite process to ensure the new processes can be successful in the centers. NASA officials have told the Academy that they will approach the rewrite in this manner.

3) Why did NAPA recommend placing counterintelligence staff in the field under ultimate supervision of the Center Director?

RESPONSE

An FBI counterintelligence assessment, completed in 2000, recommended that counterintelligence personnel be assigned to the Centers, not to HQ.¹ However, in 2007, NASA assigned the counterintelligence special agents CISAs from Center management to HQ management. This was done to centralize their control and to ensure they could devote all their time to CI matters rather than security duties. The FBI report predicted that isolation could occur if the CISAs became HQ personnel. The report also advised that if CISAs were viewed as being Center outsiders, they would not be as effective at obtaining vital CI information from Center personnel.

The NAPA study team arrived at the same conclusion as the FBI team, and found that in most Centers visited, the CISAs were not fully integrated into the Centers. Center personnel, other than the protective services personnel, often did not know the CISAs or their office locations, and could not recall any general CI training. Only a few CISAs took the initiative to meet with large numbers of Center personnel beyond travel or sponsor/escort briefings. The Panel believed that by assigning CISAs to the Centers they are more likely to fully integrate into Center activities and thereby optimize their communications with Center personnel.

NASA agreed with the Panel's assessment of the current situation regarding the CISAs but felt they could make the needed improvements while maintaining the HQ supervision of the function.

4) NAPA indicated that it is possible for NASA to make security improvements to existing foreign national access systems and realize long-term potential savings by managing its foreign national efforts in a more efficient and effective manner. Can you provide further details on what NASA needs to do to achieve such savings?

RESPONSE

To realize such savings, NASA must adopt an enterprise-wide perspective toward FNAM that capitalizes on economies of scale, shares best practices and, most importantly, streamlines the frustratingly long and inefficient process at some centers. Although the Panel did not quantify the amount that could be saved, these steps would increase the efficiency of NASA's foreign national access system, thus resulting in some long-term savings. .

¹ Ibid.

- 5) **The NAPA report recommends an Advisory Board to oversee the safety and security of NASA assets in the field. Please describe the composition of the Advisory Board and how Center and Headquarters interests would be balanced.**

RESPONSE

The task of protecting NASA's assets – its facilities, personnel, technologies, and information – is a multi-dimensional responsibility involving every NASA civil servant, contractor, and organization, as well as the support and assistance of other agencies. The successful performance of this task is dependent on completion of a number of interrelated functions – identification of assets requiring protection, accurate intelligence regarding threats, design and implementation of protective strategies, education and awareness of NASA personnel, and continuous evaluation to ensure threats are countered commensurate with their importance. This requires a comprehensive approach to risk management, employing the best practices available.

NASA needs to reconsider how it assesses and protects its information and security assets in the field. While this review has focused on FNAM, the Panel believes that a broader approach to asset protection and oversight is needed. NASA facilities, personnel, technologies, and information are highly regarded and of great interest to the world. That interest extends to some countries, governments, organizations, and individuals whose intent is to compromise those facilities, co-opt the personnel, and steal those technologies and information. While NASA currently conducts annual threat assessments at every Center by the Protective Services office, the CISAs, and the CIO, those assessments address only the areas of responsibility of those individual offices. They are not comprehensive, Center-specific assessments that consider all the elements necessary to fully protect NASA's assets.

By establishing a mechanism for comprehensive, Center-specific assessments NASA could compile threat assessments from security, CI/CT, and the CISOs into comprehensive Center and agency threat/risk assessments. This would permit HQ and Center executives to identify and prioritize vulnerable assets, assess protective strategies, allocate resources commensurate with the risk, establish and monitor controls consistent with OMB Circular A-123, and evaluate the overall asset protection efforts.

With the above considerations in mind, the Panel recommended that NASA create an Asset Protection Oversight Board to oversee the safety and security of NASA assets in the field. The overall goal of the Board is to protect all of NASA's valuable International Traffic in Arms Regulation (ITAR) and Export Administration Regulations (EAR) technical data and proprietary information, not simply the data potentially exposed to foreign nationals and to also compile threat assessments from security, CI/CT, and the CISOs into comprehensive Center and agency threat/risk assessments. The Panel also recommended that NASA create an Independent Review Team (IRT), led by the Office of Protective Services, and including membership from OIIR and CIO and field Center representatives, to biennially review all field Centers to assess and evaluate the procedural components comprising the asset protection program to also include effectiveness and efficiency. The team should operate under the guidance of the Asset Protection Oversight Board.

These assessments could be incorporated into NASA's risk management process. Specific goals and objectives for the board are listed in the "Asset Protection" narrative in Chapter 3. The Board should be supported by the HQ OPS. The structure recommended by the Panel is displayed on page 10 of this document. NASA officials have indicated to the Academy that while they support the overall function of the proposed Board, they believe it should be incorporated into existing NASA's organizational board structure.

- 6) Are the reasons advanced by NASA personnel for the inconsistent application of and compliance with established policies regarding the automated IdMAX tool indicative of insufficient awareness of risks and the absence of consequences for non-compliance? Is better training the answer?**

RESPONSE

In some cases, a lack of awareness of potential risks is definitely a contributing factor to non-compliance. The absence of consequences for "serious, preventable errors..." compounds this inconsistency. Better training is one of the key answers but it needs to be coupled with more robust IT tools and more clearly defined written instructions.

Appendix II

ADDITIONAL MATERIAL FOR THE RECORD

OPENING STATEMENT

Ranking Member Donna Edwards (D-MD)
Subcommittee on Space
Committee on Science, Space, and Technology

Joint Subcommittee Hearing
"NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information"

June 20, 2014

Good Morning, and welcome to our panel of witnesses. Mr. Chairman, thank you for calling this hearing on assessing NASA's efforts to protect sensitive information.

The legislation establishing the National Aeronautics and Space Administration, the Space Act of 1958, recognizes the importance of NASA's cooperation with other nations and groups of nations and directs NASA to *"provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof"*.

As a civil R&D agency that supports scientific research, NASA has a culture of openness, collaboration, and sharing of results. Last year, for instance, NASA approved more than 11,000 foreign national visits to its facilities and Centers and currently maintains an estimated 600 international agreements with more than 100 foreign countries, envisioning projects which may require an exchange of information to be successful.

However, the benefits of that culture of openness and sharing must be balanced with appropriate security limits and protections. Indeed, the Space Act also directs the NASA Administrator to *"establish such security requirements, restrictions, and safeguards as the Administrator deems necessary in the interest of the national security"*.

Mr. Chairman, I have often said that NASA is recognized across the world as a symbol of the United States' greatness as a nation and its leadership in science and technology. Thus, it is no surprise that so many developed and emerging nations seek to follow suit in pursuing space exploration.

Nor should it be a surprise that some may seek to obtain NASA's treasure trove of knowledge by all means possible in order to leapfrog the decades of research and billions of dollars of investment that the U.S. has made in acquiring its hard-earned capabilities.

That is why I appreciate the work completed by NASA's Office of the Inspector General, Government Accountability Office, and the National Academy of Public Administration, and their recommendations on how NASA can better protect controlled information, including export-controlled information, from unauthorized access—such as by foreign nationals.

The findings from the NASA OIG, GAO, and NAPA reports have areas of commonality. For example:

- GAO and NAPA raised concerns about the inconsistency in Center implementation of export controls, with NAPA urging NASA to take steps to reduce the decentralized authority given to Centers in implementing enterprise-wide processes. .
- The NASA OIG and NAPA found the Foreign National Access process to be overly complex and not sufficiently integrated to ensure that responsible security personnel have access to relevant information.
- Finally, GAO and NAPA both found that NASA lacks a comprehensive inventory of the types and locations of export-controlled technologies.

Corrective actions will likely be difficult for the agency to implement. We will need to be vigilant to ensure that these corrective actions do not destroy NASA's culture of openness which has proven to be a key ingredient in the agency's success.

Mr. Chairman, we have worked too hard and invested too many precious taxpayer dollars to let sensitive knowledge slip away as a result of inconsistent implementation of export controls, and so I am encouraged by the NASA Administrator's receptiveness to the recommendations made.

However, I also recognize that a sustained commitment on the part of all NASA employees and contractors will be needed for corrective actions to take hold.

I look forward to hearing from our distinguished panel, and in particular from NASA's witness, Mr. Keegan, on how NASA will address that challenge.

I yield back.

RESPONSES SUBMITTED BY NASA FOR INFORMATION REQUESTED BY CHAIRMAN BROUN

Material requested for the record on page 41, line 858, and page 45, line 944, by Chairman Broun during the June 20, 2014, NASA Security hearing.

NASA is committed to reviewing recommendations by independent evaluators such as the General Accountability Office (GAO) and to having those evaluations inform changes in the Agency's existing processes in order to better safeguard access to NASA facilities by foreign nationals and to improve the protection of sensitive technologies. The referenced GAO report as well as other recent independent investigations into export control and foreign nationals access management processes have the Administrator's personal attention and he has ordered a series of changes, to include increased employee accountability, revised Agency policies and procedures and improved employee training so as to prevent incidents like this from happening again.

The protection of sensitive technologies is the personal responsibility of all NASA employees and a responsibility that every NASA manager, up to and including the Administrator himself, takes very seriously. Therefore, in May 2014, Administrator Bolden directly addressed those officials from across the Agency who manage the implementation of NASA's Export Control Program about the critical role they play in safeguarding sensitive NASA technologies. He also issued a communication to all NASA employees reminding them of their responsibility to comply with all export control regulations and foreign national access management requirements. His message stressed that safeguarding sensitive information is a serious matter and that penalties for noncompliance can include fines and imprisonment, as well as administrative personnel actions, such as reduction-in-grade or even termination.

It is important to note that the recent independent reviews conducted by the GAO, the National Academy of Public Administration (NAPA) and NASA's own Inspector General's Office did not identify any instances when NASA employees maliciously bypassed export-control restrictions, thereby violating Federal laws, nor did they document any occurrences of NASA employees purposefully sharing sensitive information with foreign nationals. Instead, the independent reviews identified instances of employee carelessness and poor judgment with respect to export-control and foreign national access procedures at NASA Centers, which led to policy and procedural violations. These findings resulted mostly from employee confusion regarding individual roles and responsibilities in the export control and foreign national access management process. Given this confusion, Administrator Bolden directed Associate Administrator Lightfoot to assess these independent review findings and to recommend any potential corrective action in terms of Agency policies and procedures with regard to these findings. Additionally, instances of alleged violation of Agency policies by specific NASA employees have been and will be handled administratively using established disciplinary processes.

Material requested for the record on page 63, line 1405, by Congressman Johnson during the June 20, 2014, NASA Security hearing.

NASA is committed to reviewing recommendations by independent evaluators such as the General Accountability Office (GAO) and to having those evaluations inform changes in the Agency's existing processes in order to better safeguard access to NASA facilities by foreign nationals and to improve the protection of sensitive technologies. The referenced GAO report as well as other recent independent investigations into export control and foreign nationals access management processes have the Administrator's personal attention and he has ordered a series of changes, to include increased employee accountability, revised Agency policies and procedures and improved employee training so as to prevent incidents like this from happening again.

The protection of sensitive technologies is the personal responsibility of all NASA employees and a responsibility that every NASA manager, up to and including the Administrator himself, takes very seriously. Therefore, in May 2014, Administrator Bolden directly addressed those officials from across the Agency who manage the implementation of NASA's Export Control Program about the critical role they play in safeguarding sensitive NASA technologies. He also issued a communication to all NASA employees reminding them of their responsibility to comply with all export control regulations and foreign national access management requirements. His message stressed that safeguarding sensitive information is a serious matter and that penalties for noncompliance can include fines and imprisonment, as well as administrative personnel actions, such as reduction-in-grade or even termination.

It is important to note that the recent independent reviews conducted by the GAO, the National Academy of Public Administration (NAPA) and NASA's own Inspector General's Office did not identify any instances when NASA employees maliciously bypassed export-control restrictions, thereby violating Federal laws, nor did they document any occurrences of NASA employees purposefully sharing sensitive information with foreign nationals. Instead, the independent reviews identified instances of employee carelessness and poor judgment with respect to export-control and foreign national access procedures at NASA Centers, which led to policy and procedural violations. These findings resulted mostly from employee confusion regarding individual roles and responsibilities in the export control and foreign national access management process. Given this confusion, Administrator Bolden directed Associate Administrator Lightfoot to assess these independent review findings and to recommend any potential corrective action in terms of Agency policies and procedures with regard to these findings. Additionally, instances of alleged violation of Agency policies by specific NASA employees have been and will be handled administratively using established disciplinary processes.