[H.A.S.C. No. 113–46]

PAST, PRESENT, AND FUTURE IRREGULAR WARFARE CHALLENGES: PRIVATE SECTOR PERSPECTIVES

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

HEARING HELD
JUNE 28, 2013

U.S. GOVERNMENT PRINTING OFFICE
82–461 WASHINGTON : 2013

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

MAC THORNBERRY, Texas, *Chairman*

JEFF MILLER, Florida
JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
RICHARD B. NUGENT, Florida
TRENT FRANKS, Arizona
DUNCAN HUNTER, California
CHRISTOPHER P. GIBSON, New York
VICKY HARTZLER, Missouri
JOSEPH J. HECK, Nevada

JAMES R. LANGEVIN, Rhode Island
SUSAN A. DAVIS, California
HENRY C. "HANK" JOHNSON, JR., Georgia
ANDRÉ CARSON, Indiana
DANIEL B. MAFFEI, New York
DEREK KILMER, Washington
JOAQUIN CASTRO, Texas
SCOTT H. PETERS, California

PETER VILLANO, *Professional Staff Member*
MARK LEWIS, *Professional Staff Member*
JULIE HERBERT, *Clerk*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2013

FRIDAY, JUNE 28, 2013

PAST, PRESENT, AND FUTURE IRREGULAR WARFARE CHALLENGES: PRIVATE SECTOR PERSPECTIVES

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

PAST, PRESENT, AND FUTURE IRREGULAR WARFARE CHALLENGES: PRIVATE SECTOR PERSPECTIVES

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES,
Washington, DC, Friday, June 28, 2013.

The subcommittee met, pursuant to call, at 10 a.m., in room 2118, Rayburn House Office Building, Hon. Mac Thornberry (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MAC THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

Mr. THORNBERRY. The subcommittee will come to order. We are going to be interrupted by votes here shortly, so we are trying to make the best of a difficult situation.

I will just say that it has been a continuing interest of this subcommittee on the lessons learned from irregular warfare and how we go forward. And so today's hearing is an attempt to get a cross-section of private-sector opinion about that subject, and we very much appreciate the witnesses being here and, in advance, your patience in a rather constrained day.

With that I yield to the ranking member, Mr. Langevin.

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank our witnesses for being here; thank the chairman for holding this hearing. In interest of time and brevity, in light of the fact that we will be pulling votes, I will submit my opening statement for the record, but again thank our witnesses for being here.

I yield back, Mr. Chairman.

Mr. THORNBERRY. Thank you. Let me turn it over to our witnesses: Mr. Rudy Atallah, Chief Executive Officer of White Mountain Research; Mr. Mark Cohn, Vice President, Engineering and Chief Technology Officer for Unisys Federal Systems; Barry Costa, Director, Technology Transfer, The MITRE Corporation; and Scott Jacobs, President of New Century US. Again thank you all for being here.

We will turn it over to you, and, without objection, your entire written statement will be made part of the record, and we will turn it to you to summarize your statement, if you will. Mr. Atallah.

STATEMENT OF RUDOLPH ATALLAH, CHIEF EXECUTIVE OFFICER, WHITE MOUNTAIN RESEARCH LLC

Mr. ATALLAH. Mr. Chairman, honorable members of the subcommittee, thank you for the invitation. Let me just dive right in and outline a few of my thoughts.

I'm going to start by discussing a few points on the challenges to irregular warfare as we see it from our side, from my company. The first challenge is understanding non-Western friends and foes. Perhaps the greatest challenge to IW [irregular warfare] observed since 9/11 attacks is our inability to accurately understand and therefore project how and why nonstate allies and adversaries, including those inspired by militant strands of political Islam, think, organize, and operate.

Part of this problem set arises from our institutional tendencies towards mirror imaging; that is, thinking like professional soldiers, analysts, and policymakers rather than non-Western activists, bureaucrats, or militants, motivated as much by identity belief or cultural imperatives as they are by traditional notions and strategy.

Challenge number two is our overreliance on technology. Despite recognition since 9/11 of the importance of sociocultural understanding, the reality of our approach to IW remains focused on zeroes and ones. We continue to rely increasingly on intelligence derived from technical sources and less on humans. Context derived from understanding and thinking like others takes a back seat to information.

Beyond the monetary burden associated with overreliance on warfighting technologies, our ability to grasp and contend with complex sociocultural issues is gradually eroded. Our soldiers have grown accustomed to possessing enormous amounts of intelligence data at their fingertips that provide answers to almost every question arising within the operating environments. But whether the financial resources required to sustain this technology will be there in the coming lean years is unknown.

SOF [special operations forces] units will have to return to more traditional modes of working as small units conducting operations by, with and through local military liaison forces and other local surrogates. Although advanced technologies will certainly play a role in these cases, these small units will succeed or fail based on their ability to analyze, fight, and navigate within the local environment.

The third challenge is defining the political outcomes of IW. It is a well-known maxim that war is politics by other means. A clear understanding of our objectives and strategies in waging IW is essential, essentially given the primacy of influence and winning at war's moral level. Further, the clear articulations of these objectives, basically our desired end state, to the American public is also key, given this necessity to generate support for the long-term operations and patience that characterize effective irregular warfare.

Fourth, our fourth challenge is limited to SME [subject matter expertise] immersions. Another apparent challenge in combating irregular warfare is basically having a lack of reliable subject matter expertise in some regions of the world. Generating a meaningful understanding of a country or a region's sociocultural issues requires years of immersion.

It has been our observation that when DOD [Department of Defense] reacts to a new issue, it often reaches out to academia for answers. However, it is often the case that academic advisors have limited understanding of ground-truth sociocultural context because their expertise is gleaned from desktop research or coupled with trips to a distant capital. Instead of turning to individuals who have spent meaningful time on the ground conducting field work and developing objective, qualitative perspectives on the challenges at hand, DOD too often invests in shallow and often biased expert opinions. The result is poor, often skewed understanding of both the problem set and the environment that is nevertheless translated into IW planning.

Recommendations. First, we need to expand our human capabilities. As American warfighters, we will always have the ability to do something, but having good intelligence coupled with solid context allows to us do the right thing.

Second, we need to couple an expanded HUMINT [human intelligence] capability with new methods of sociocultural training and alternative analysis programs that promote viewing the environment through the eyes of non-Westerners.

Third, continued private-sector partnerships as well as—are essential for DOD. Businesses like White Mountain Research that work overseas have a great deal to offer as the market forces us to stay in tune with foreign political and sociocultural issues in order to compete. As we conduct our peer-to-peer research and keep pace with local politics in foreign countries, DOD can gain richly from our experience.

Fourth, we must bear in mind everything has an economic limitation. Based on this, at the political level we should determine what we want our objectives to look like and define and calibrate appropriate IW resources to meet it.

Fifth, the lack of continuity in DOD must be addressed. Most soldiers never exceed more than 2 to 3 years in an overseas assignment. This does not allow for sustained familiarity with the host country that is so crucial in IW. This is why programs like AFPAK [Afghanistan-Pakistan] Hands must be continued and expanded to other regions of the world. These programs can dovetail well with regional centers of excellence, like the Africa Center for Strategic Studies or the George C. Marshall Center.

Finally, I will conclude with that more effective and systemic screening procedures should be instituted for academic advisors. These should be vetted for not only their subject matter and knowledge, but also their objectivity. When advising on a far-flung place like Mali, Nigeria, extensive on-the-ground experience should also be a prerequisite before there are any people put in position to educate the warfighters. We have witnessed too many times the unfortunate consequences of unprepared or biased advisors hired to provide direction to crucial DOD initiatives.

Thank you.

[The prepared statement of Mr. Atallah can be found in the Appendix on page 29.]

Mr. THORNBERRY. Thank you.

Mr. Cohn.

STATEMENT OF MARK COHN, VICE PRESIDENT, ENGINEERING AND CHIEF TECHNOLOGY OFFICER, UNISYS FEDERAL SYSTEMS

Mr. COHN. Good morning.

Mr. THORNBERRY. Hit the button and get closer.

Mr. COHN. Thank you very much.

Good morning, Chairman Thornberry, Ranking Member Langevin and other distinguished members of subcommittee. I am Mark Cohn, Chief Technology Officer for Unisys in our Federal Systems division. We thank you for inviting Unisys to participate in this hearing about lessons learned in irregular warfare challenges in today's operating environments and how industry can contribute to enhancing our security.

Around the world and here at home, Unisys is a leading provider of integrated security solutions, many of which incorporate advanced biometric and identity management technologies. For example, we delivered a national identity system for Angola with multiple biometrics that required mobile enrollment in the villages under austere conditions. It provides counterfeit-resistant proof of identity to a widely dispersed population, representing a cornerstone of citizenship in this emerging democracy as proof of their right to vote and for access to government services.

Recently we delivered a system for Mexico that provides for storage of 110 million identity records, comprising fingerprints, iris scans, and facial images, with a capacity to accept 250,000 enrollments daily.

To defend the Nation and defeat our adversaries engaged in irregular warfare, the Defense Department requires capabilities in counterinsurgency, counterterrorism, foreign internal defense, and stability operations. Success depends on separating enemy combatants from the civilian population or the innocent members of the civilian population.

Biometrics can be used to record the identity of enemy combatants, to link individuals to events such as IED [improvised explosive device] explosions. So in irregular warfare, a primary U.S. objective is also to create a safe and secure environment for friendly populations and friendly military forces to mitigate disruptions to their daily lives. Providing that safe environment is complex as the enemy is generally well concealed within the population.

Another challenge in irregular warfare is being able to distinguish loyal indigenous security forces from disloyal foes who can procure uniforms and equipment that allow them to blend with regular forces and conduct surprise attacks in installations or within government buildings.

It is important to recognize there are limitations to the biometric systems and methods available to U.S. military forces in theater. Data capture generally requires close physical proximity to a subject who is usually uncooperative, and relies on equipment and a system architecture that reportedly fails at times to meet vital needs.

Today's tactical collection equipment employs custom-built integrated mobile kits that can be bulky and cumbersome, and there are problems with data synchronization. Industry can help by taking advantage of new mobile processing platforms derived from

consumer mobile devices extended with ruggedized biometric sensors, and by implementing interfaces in a unified architecture that streamlines uploads to the authoritative database so it can return match/no-match results to the operators quickly.

It is essential that transmitted and stored identity information and biometrics stay coupled, because separation of the data undermines the system's speed, accuracy, and ability to detect enemy combatants.

The relative cost and performance of biometric systems has improved dramatically in the last 12 years. There is greater reliance on multiple biometrics that can interoperate between vendors. There are multiple examples of large-scale systems implemented rapidly at predictable cost because we used a framework of proven components. That enables us to deliver systems that are flexible, scalable, secure; to utilize multiple workflows and biometric modalities without complex custom software coding; and to be extensible through standards-compliant open interfaces.

There has also been a great expansion in the diversity of use cases for biometrics. For example, in Canada we implemented a system for the Port of Halifax that uses vascular, that is vein pattern recognition, for access to the port's 5,000 workers. We did the restricted area identity card that uses fingerprints and iris scans to secure Canada's 28 major airports.

In all regions of the world we see widespread consumer acceptance of biometrics. There is significant commercial interest in banking and other regulated industries because biometrics can simplify the user experience while increasing security when compared with passwords and PINs [personal identification number].

The Department of Defense today employs a user authentication approach that relies on a common access card and a PIN. This is highly secure, but can be impractical. A commercially available biometrics-driven alternative used today in the banking industry is more convenient, less expensive and time-consuming to administer, eliminates the problem of transport and lockout during PIN reset, and can address risks that the current CAC [common access card] and PIN model cannot, such as the impostor threat.

So in conclusion, we believe the Department of Defense can expect these international and industry developments are in many cases applicable to the challenges confronted in irregular warfare, and we think they can help improve internal security and stability through U.S. and partner-country initiatives. Unisys looks forward to supporting that progress both here and overseas.

Thank you.

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

Mr. THORNBERRY. Thank you.

Mr. Costa, I think we have time to get your opening comments.

STATEMENT OF BARRY COSTA, DIRECTOR, TECHNOLOGY TRANSFER, THE MITRE CORPORATION

Mr. COSTA. Chairman, Mr. Langevin, and members of the subcommittee, thank you for inviting me today to speak about irregular warfare challenges, specifically in my case the value of sociocultural situational awareness and the technologies and data

that enable such awareness and support rapid and effective decisionmaking.

What I will describe is 21st-century radar, technology that can provide us with rapid and effective insight into the changing human terrain for irregular warfare as well as other missions. Just like an airborne camera allows us a view of the physical terrain, and infrared lets us see into the night, there are now technologies that allow us a view of the human terrain to include populations, networks, groups, and behaviors.

The Nation must adapt its methods and create tools that reflect the realities of national security in a new age of real-time global information flow, and we must understand and engage in the public dialogue created by these new communication media. As demonstrated by the swift changes brought about by the Arab Spring, we must rapidly sense, understand, and, if necessary, engage with words and deeds to positively shape the environment.

While technology can't replace deep human insight, we believe that empirically derived, scientifically grounded technologies can help us understand the human terrain. The defense community has built a science and technology foundation necessary for studying and understanding sociocultural behavior. Given that this technology foundation allows us insight into the human terrain, we are now better positioned to pursue effective courses of action in the full range of military operations.

These new technologies are enablers for irregular warfare, allowing us to identify extremist networks, groups, and key influencers. Additionally, these technologies support our analysts and decisionmakers as they work to mitigate irregular warfare threats.

Much remains to be done to evolve and adapt these sense-making capabilities to play a vital role in current and future missions. Recent rapid and profound shifts in the geopolitical context have brought renewed attention to challenges such as hostile nonstate actors who may be pursuing weapons of mass destruction, nation-state instability driven by drug economies and transnational criminal issues, humanitarian and disaster relief, and cyber threats. These technologies can give us some more nuanced insight into global challenges, but this is just the beginning, and continued research is likely to make significant additional progress.

However, we must conduct such research with a keen eye toward quick and effective transitions to those warfighters, programs and organizations that need them. While there are many difficult challenges in this area, some of which will take years to solve, there are technologies and methods available today that can help us find key information within this deluge of data and understand the effectiveness of our words and actions upon those with whom we engage.

Experience to date suggests an exciting future in which global information, applied research and analytics are fully and dynamically integrated; however, DOD and the Nation are not yet at that desired end state. To get closer, DOD should maintain the momentum created over the past several years by supporting promising research that will enable the capabilities most relevant to future national security demands.

Let me leave you with this thought: If DOD had ended its research investment in traditional radar technologies after just 5 years, the program would have ended around 1939, leaving us with a rudimentary and tantalizing potential for long-range sensing. Social radar is at that tantalizing stage, and we can see the promise. Drones and satellites alone can't detect violent speech or determine how our adversaries' narrative is spreading. We need a global and persistent indications and warning capability. We call that social radar.

[The prepared statement of Mr. Costa can be found in the Appendix on page 50.]

Mr. THORNBERRY. Thank you.

Mr. Jacobs, if you don't mind, I think we will go ahead and take your opening statement. Now, there are still 356 Members who haven't voted yet, so I think we will have time to do that, and then we will come back for questions.

STATEMENT OF SCOTT E. JACOBS, PRESIDENT, NEW CENTURY US

Mr. JACOBS. Thank you, Mr. Chairman, Ranking Member Langevin, members of the subcommittee. I thank you for your opportunity to appear before this panel today. And as a retired NCIS [Naval Criminal Investigative Service] special agent and a graduate of the Congressional Fellowship Program, I am acutely familiar with the leadership that this committee does every day, and it is that leadership that is vital to our Nation's security.

New Century US is a privately held firm that is the American subsidiary of the London-based New Century International. Currently our firm is executing a contract with the U.S. Government to provide training that supports the professionalization of the Afghan National Army, while New Century International continues to provide training and mentoring to the Afghan National Police and the Afghan National Army in support of the NATO [North Atlantic Treaty Organization] mission in Afghanistan. In short, our programs and the collective experience of New Century personnel has positioned our firm as both the keen observer of irregular challenges worldwide and as a knowledgeable proponent of irregular solutions.

At New Century we believe a focus on improving the capacity of the Afghan military and security forces and other host nation security forces is a wise, cost-effective and intelligent investment for supporting American foreign policy objectives because it offers a potential to build an effective leave-behind and self-sustaining indigenous security force after a large-scale U.S. military presence is reduced or becomes unavailable.

With that in mind, our firm's flagship program is called Legacy and was first implemented in western Iraq province of al Anbar in 2008, and is currently being executed in Afghanistan. Aimed at improving the capability and capacity of the ANP [Afghan National Police] and ANA [Afghan National Army] forces, the current iteration of Legacy employs a specific doctrine and teaching methodology that is based on the experience of the British constabulary force, or Special Branch, in Northern Ireland during the conflict in the 1970s and 1980s.

The value added of New Century approach lies in the methodology, but also of the deep experience found within the ranks of the personnel that work for New Century. These are former Royal Ulster Constabulary police officers that have worked tirelessly in Northern Ireland to defeat and disrupt the networks that perpetrated the violence in Northern Ireland.

Since irregular threats abroad and Federal budget pressures at home are almost certain to continue, we believe the indirect and irregular approach will become increasingly important in the days ahead. That is why our firm embraces and supports the all-important "by, with, and through" creed of the Special Operation Force community as it applies to achieving U.S. foreign policy objectives.

We view this indirect approach as practical and essential for working with foreign allies as well as for identifying and confronting irregular challenges around the globe, especially in environments requiring a limited counterinsurgency response or, as Admiral McRaven would say, a small footprint. Therefore, establishing carefully targeted assisted programs to develop and empower the local authorities of American allies would be wise.

Just imagine America's strategic position if we were able to establish indigenous-led counterterrorism COIN [counterinsurgency] programs in states that struggle to defeat irregular networks. Imagine, too, the improved security posture and greater moral authority of America if both the State Department and the Department of Defense would combine efforts and jointly offer assessments to potential partners and allies.

Three lessons learned that I would like to talk today that we have learned in Afghanistan. One, Special Branch-like activities to ultimately succeed need the U.S. military. The U.S. military must provide daily support to overall COIN doctrine and strategy. They must train for it, they must develop doctrine for it, and this must be embedded in the very mindset of how we wage war.

Effective COIN efforts take time. We learned in Northern Ireland that it took over 20 years to penetrate the criminal networks that promoted the violence in Northern Ireland. It takes time.

And final observation is actually a concern and pertains to the point just made about doctrine, training, and budgeting. Despite significant gains in the field, notwithstanding the 2008 issuance of the DOD Directive 3000.07, the Department and each of the military services have remained somewhat listless with respect to this important subject. The 2008 directive assigned additional duties to SOLIC, the Special Operations/Low-Intensity Conflict Office of the Assistant Secretary of Defense, for organizing lead roles defining, and guiding, and coordinating irregular warfare-related activities across DOD. Yet 5 years later we still do not see any tangible leadership on these issues anywhere in the Department. The 2010 Quadrennial Defense Review and the 2012 Defense Strategic Guidance only lightly referenced the concept, and no true champion, no true champion has emerged for institutionalizing such lessons or for providing a sustainable budget.

And I must point out—I know I am just about out of time, but this is a very critical point. General Stan McChrystal recently talked about it takes a network to defeat a network, going back to earlier comments of Mr. Atallah as well. And ironically this com-

mittee echoed his comments back in the 2011 and 2012 National Defense Authorization Acts, an important point, where you praise the approach of the Legacy program in the committee report. And also the report noted special interest in the "attack of the network" approach. And you made two recommendations. Actually you directed the Secretary to provide you with two things: the applicability of Legacy program in other operations and regions where network-based threats are present, or where conditions are conducive to supporting these threats; and number two, very important point, options for an appropriate management structure within the Department to institutionalize and sustain the capabilities that Legacy and, I must emphasize, similar programs provide to the warfighter.

And finally, in conclusion, we agree with both General McChrystal's assessment and your wise words after toiling years in the field doing this kind of capacity building, but we need a more visionary and effective leadership in the United States Government, just as more international partners and allies are required. Our Nation cannot do it alone. It simply cannot. "By, with, and through" is an effective guiding principle for the United States in the years ahead. Our recommendation is for us to follow it.

Thank you very much, and I look forward to your questions.

[The prepared statement of Mr. Jacobs can be found in the Appendix on page 62.]

Mr. THORNBERRY. Thank you all. Lots of interesting topics to follow up on. We will stand in recess while we vote, and they are estimating it will be about 45 minutes, so Pete will buy you all a cup of coffee in the back.

Thanks, Pete.

[Recess.]

Mr. THORNBERRY. The subcommittee will come to order. Thank you all again for your patience. I think Mr. Langevin had another meeting he was going to try to grab, and then will try to be back with us.

Let me go back to, as I say, each of you made a number of interesting points. Mr. Atallah, you said in your testimony—or one of the points you made is there is an overreliance on technology, and yet we talk about human terrain radar, which I am not exactly sure what that is, but I presume there is a technological component of that. The kinds of things we hear about are monitoring social media, for example, and detecting trends and that sort of thing.

So I guess I would appreciate thoughts from each of you about this, I guess, question: Are we too dependent on technology, and are we looking to technology to solve what may be nontechnological problems?

Mr. ATALLAH. Mr. Chairman, thank you very much for your question. I had to think long and hard about this, and, yes, we do rely heavily on technology, and I find it more with our younger generation that is actually entering the forces, they can't function without their devices.

I am an Africanist. I spend a lot of time on the continent. And although cell phone technology, for example, on the continent is growing pretty quickly, there are remote areas in Mali, Niger, different places where various ethnic groups are not relying—don't

use technology. So how do we metric those individuals? How do we figure out what those individuals are doing? So we come back to we are looking for solutions on Facebook or Twitter just to see what these individuals are doing, and we miss the important part.

I think what we need to do is focus more on the basics. HUMINT, I pushed for that. Sociocultural training is important. We do a little bit of it, but we don't get into the depth that is required in order to understand. I was born and raised in Lebanon. When I understand a culture from its roots, and I speak the language, the last thing I want to do is go to technology to look for an answer. The first thing I want to do is to go to a human being that I know down the street that may have the answer. And that is where we are starting to miss the boat. We find ourselves today just sitting 7-, 8,000 miles away looking for an answer that is in front of us on a screen instead of having that granular HUMINT side that is important.

Mr. COSTA. Sir, I agree that deep human insight is required, and I agree that people like Mr. Atallah can't be replaced, but on the other hand, there are technologies that allow insight to him, to people like him, and to others, decisionmakers included, that can allow us to understand trends. Four billion, eight hundred million people have a cell phone right now, and most of the world will have a cell phone and be wired, wired so to speak, within the next decade. It is a lot of information that people are generating, that they are discussing on social media and in other forums, and that dialogue becomes increasingly important.

It is not the only source. There are lots of other great data sources. There are lots of other great technologies and methods. But I would suggest that understanding this emerging dialogue and using these technologies to help foster understanding is critical. And there have been some great examples of successes doing that, but, again, it doesn't supplant just deep human understanding that people like Mr. Atallah can provide.

Mr. THORNBERRY. When you talk about human terrain radar, what sorts of things are you talking about?

Mr. COSTA. A variety of technologies, sentiment analysis is one of them, emotion analysis is another one; technologies that model decisionmaking, others—technologies that even forecast instability. There is a system in use in the Department of Defense right now that forecasts long-term instability. So, as an example, will government X or will country X experience instability events in the next 6 months? There is a system that does that right now. It is not perfect; however, it provides deep insight to analysts studying that country and allows them to dig deeper into issues of interest. So those are the sorts of technologies that I am referring to.

Mr. THORNBERRY. Mr. Cohn, if you all are putting in these ID [identification] cards in a variety of countries that don't have maybe as much technology as we do, what are some of the challenges that you have run into in implementing those technologies?

Mr. COHN. Thank you, Mr. Chairman. It is an interesting subject that fascinates us in the industry. I could probably spend an hour talking about that, but I would like to keep it brief, though.

There are a number of sociocultural issues that we encounter that are quite striking. In Malaysia, where we happen to do the na-

tional ID, in that country they have religion that appears on the face of their ID card, which seemed like a pretty oddball concept to those of us. They happen to also have a default state religion that goes on there if you don't claim one. It is a different world.

In the Middle East, where we do a lot of work, and Malaysia is one of the countries where this arises also, there are cultural concerns regarding how we enroll biometrics because of personal privacy. If you have a fingerprint sensor, and you use both hands, there is a tremendous aversion regarding hygiene. Therefore iris is used, say, for the expellee database [National Expellees Tracking and Border Control System] from the United Arab Emirates because you can still take a sample with a veil.

So we see a lot of variation, and in candor, without getting down in the weeds regarding this sort of cottage industry of biometrics, the way we see it, it has to be tuned to the country and its culture. But the Prime Minister of Malaysia said in 1995, this will be a way that we catapult our country into the 21st century. They saw it as a big part of modernizing their economy, that they could have more participation because biometric verification would then be an inexpensive, widespread social good.

When Pay By Touch, a U.S. company, went into bankruptcy, Singapore banks could no longer use fingerprint verification for banking. Malaysian banks that used to thumbprint under MyKad, their national ID card, could continue to do banking security with biometrics. The banks there have a key to unlock the card, and you can put your equivalent of an ATM [automated teller machine] card onto the same card the government issues, and they have a local e-Purse application so you don't have to carry cash when you go to their equivalent of a 7-Eleven. So in other words, this allows people to participate in a modern economy in a way that we don't even think of in this country. And I could go on about some of the Latin American differences as well whenever you would like.

Mr. THORNBERRY. Mr. Jacobs, can you reflect on technology and how it has applied, and the challenges, I guess. You talked about training the Afghan National Army. I would presume in Afghanistan you run into some of those as well.

Mr. JACOBS. Absolutely.

I would first like to go back to the question you asked Mr. Atallah here. The purpose of the Legacy program is to penetrate a network, the criminal network, drug network, terrorist network. And then through that penetration how you do that is by developing sources, informants, and tasking informants to get information. And then based upon that information, you do something with it; you take action against that network to disrupt it. And a person can do that.

You can ask a person for information. You can task him to do something. It is hard to task a technical device. And even though technical devices are added benefits, and can certainly help us in our endeavors, it is the human piece that, in my years of experience, have really been deemphasized in terms of our, you know, national strategy. It is more of a reliance on the technical piece, and the very human piece, the human interaction, the relationship development piece is what I believe has been shortchanged in the most recent history. But it is that human piece that allows us to

penetrate the networks that do these bad things that harm our country. So the challenge, and it is a challenge, is how do you take the good technology and apply it to the human piece, and that is a challenge.

In terms of Afghanistan, I had just recently come back from Afghanistan, and I was talking to an Afghan Army general about GEOINT capability—geospatial intelligence—and what were their requirements for this capability. And he was a very practical general, he had he fought the Russians during the Russian incursion into their country, and he said, Scott, what I need is a good map. You know, I don't need the GEOINT capability. You know, I need a good map, and then I need your help in training the map readers. And again, he focuses on the human piece, you know, an individual utilizing a map, and from that map you do your targeting, you do your operational planning.

And I thought that was very insightful from an Afghan general that has the ability to get GEOINT, but he says, no, I can't sustain it. There is not a legacy here. My people don't understand how to work GEOINT because of my lack of education here.

So you have to build systems at a level in which the host country can apply it. And that is the lesson that we have learned through Legacy and through other experiences that I have had in my career.

Mr. THORNBERRY. Switching topics, in your written and in your oral testimony, you talked about the importance of DOD, and State, Intelligence Community working together, that interagency cooperation. Can you offer your thoughts on where we are and if you have a suggestion on how that—what can be done to improve that moving ahead. And actually for any of you who would offer your insights based on your experience about how well the Federal Government works with itself, and how well the Federal Government takes advantage of the opportunities the private sector offers.

Mr. JACOBS. Thank you for the question, Mr. Chairman.

The State Department and the Department of Defense have enormous resources, personal resources, training capabilities, but oftentimes there is—because of the lack of coordination between the different parts of the Government, and oftentimes the same purpose, we see an ability not to fully leverage those resources that both State and both DOD have.

In many countries that I have been in, you don't have an effective police force, and your military force is that police force, and so you have to use irregular techniques to train a military component. But the problem with the military is that the U.S. military is not a police capability; that resides in the State Department. And so that is where this cross-pollination could really be an effective tool to more accurately and appropriately teach police skill sets to the military component on the ground.

So that is really what I mean about blending in certain environments that we find ourselves in today where that leverage would be a powerful U.S., you know, strategy to work together to get more done on the ground.

Mr. THORNBERRY. Okay.

Mr. COSTA. Chairman, within my domain we have found that technology itself can be a point of agreement. And we have used

one of the systems that was developed by the Assistant Secretary of Defense for Research and Engineering called the Integrated Crisis Early Warning System as a rallying mechanism to bring both the IC [Intelligence Community] and the State Department together, in a limited sense at least, around some technology that actually does help them forecast and understand data. That in itself has created a dialogue which is very, very productive. And in addition, using this allows them to more fully leverage private industry since some of this technology is commercialized, and they are bringing this to bear.

So MITRE, as a nonprofit FFRDC [federally funded research and development center], is helping support this and bringing the world to bear in support of these problems. And technology is one way that we believe we can bring it together, and we are.

Mr. COHN. Sir, we have seen actually what I would characterize as excellent cooperation in the areas that we get to observe. And perhaps I should explain that. Coming at this from the perspective of this identity management challenge, our biggest concern is how do we collect information about the largest group of the population in a cooperative way, because it is a lot cheaper and easier to get them to cooperate. So we want a national government or equivalent to create some kind of a use case where the citizens voluntarily benefit from participating, that allows us to kind of deal with the "needles in haystack" problem. Those that comply, it is cheaper for us to have that data collected by a friendly government, so if whatever sensitivity they need to the local culture, the State Department, the community, and Defense Department all see the benefit of this, and the programs that we have, I believe, are cooperative in this space.

Ultimately there is a shared interest with the ally abroad to share information that can be useful, denying movement to adversaries, be able to some degree even target the enemy. And it benefits us if we don't have to do the work ourselves, using a Western perspective with our local footprint, but rather have them, in a sense, helping us, but by dealing with a lot of the data collection and even the analysis in many cases.

But if I can return just to the general issue, you know, in terms of technology versus HUMINT, I don't think that is really a choice we must make. We will all be living in a world where technology continues to flourish around us. If we fail to take advantage of mobile computing, of analytics that are available to both our adversaries and us, to cloud-based repositories that assemble more and more information together, then shame on us for failing to do that. On the other hand, that is not a substitute for people on the ground, and I don't think it is really a choice that we make directly.

Mr. THORNBERRY. Very well.

Mr. ATALLAH. Mr. Chairman, with respect to everybody, I am not denying that technology doesn't have its uses obviously, and I think everybody has said that.

And in terms of your question on interagency cooperation, I think from my experience interagency cooperation is very good whenever we are focusing on something kinetic. We tend to come together and make solid decisions.

I think where the interagency still lacks is when it is nonkinetic. Decisions are often mired in disagreements, and the approach between the various organizations sometimes slows to a halt, and therefore it takes a long time to come up with a decision on a particular problem set.

And I think if we can take best practices from how we come together in coordinating on a kinetic strike and apply them to nonkinetic issues, I think that is where we can see ourselves moving forward.

I find this, again from an African perspective across the continent, I have seen this time and time again from my days in OSD [Office of the Secretary of Defense], and now as an outsider working on the corporate side trying to support certain agencies and looking at some of the key issues focused on CT [counterterrorism].

Mr. THORNBERRY. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Again I want to thank our panel of witnesses for being here today and for your testimony.

Before I give my questions, I don't know if he had been acknowledged already, but I know the subcommittee has had its jurisdiction expanded, adjusted over the last several years, but in another incarnation the former chairman of this subcommittee Mr. Saxton is in the audience, Jim Saxton. I just wanted to welcome you, Mr. Chairman. It is great to have you here.

With that, if I could just turn to our witnesses. I am going to start with Mr. Cohn, but if others to like to chime in as well. You touched upon this in your testimony, but again, if you could speak more broadly about the capabilities that biometrics and defense forensics bring to an irregular warfare environment, and how useful are those capabilities in a more conventional fight?

Mr. COHN. Thank you. I appreciate the question.

We focus a lot of attention on identification technology with respect to live samples that we get from people that we encounter in real life. That tends to be the economic engine that drives us forward. DNA [deoxyribonucleic acid] indexing happens to be one of the biometrics that isn't normally used that way because you don't get a rapid response. Today it is not available in real time.

But DNA is a biometric. We have, in my company, done the algorithm development work and rehosting for CODIS [Combined DNA Index System] for the FBI [Federal Bureau of Investigation], and so we have some experience with that. We have designed some of the kinship analysis protocols, and that can play a big role when trying to sort out friend from foe even when you don't have a sample from an individual. If tribal affiliation is a factor in someone's loyalty, that is one of the things you can, in fact, tell from DNA. You also can do disaster victim identification, identifying remains based upon relatives, using kinship analysis.

So biometrics has a broader set of use cases than just verification of identity for willing subjects. But ultimately most of the use cases that we think about commercially involve witting subjects who are cooperative. In warfare we are going to be in the opposite scenario for the most part. And there have been emerging technologies like three-dimensional face verification, which we can use at a distance exceeding 20 meters now to be able to identify with great accuracy and biometric precision almost at the level of iris recognition,

which means that we are dealing with accuracy at the level of tens of millions in terms of our discrimination ability. So we could have standoff distances, protect facilities that way.

We also have something called two-and-a-half dimensional face, which may seem a little bit odd, where they can use a 2D [two-dimensional] facial gallery, compare it to unposed, uncontrolled poses in the crowd. We do it for soccer hooligan detection in Europe. We might as well do it at IED scenes, where we could capture passively images of people around, associate them with the images captured at other scenes to be able to build a model of whoever you encounter on a frequent basis. But those might be examples of biometrics, not civilian use, but where they might be used in——

Mr. LANGEVIN. The last, the facial recognition technology, the two-dimensional images, how quickly does that happen? How rapidly can you find a cross-check?

Mr. COHN. Oh, the matching algorithms are fast enough so that you could determine if somebody is on a known, say watch list of a magnitude equivalent to our national watch list, in real time. In candor, it is not so much the elapsed time, it is the number of processors you have behind the scenes to be doing those checks in parallel against the known repository. So it may be that if we are talking about a tactical scene, that processing may be done by server cluster, if you will, not on board, say, the mobile vehicle where the cameras and sensors reside, if that makes sense.

Mr. LANGEVIN. Anybody else care to comment on biometrics?

Mr. JACOBS. I would like to comment very briefly. I think when you use biometrics, you have to have really a good domain awareness, what is the technical capability on the ground of that population. And the reason for that is so you know what to use in terms of technology to get the kind of information that you need. I think that is an important point here.

Mr. LANGEVIN. Thank you.

So for the panel, what partner-nation training capabilities are particularly suited in your views to be resident in DOD or in industry, particularly with regard to cybersecurity?

Mr. COHN. Sir, I am probably the closest person to a cybersecurity person here on the panel, so I will thank you for the question because it is so important to our society and to our partner nations.

DOD, through NSA [National Security Agency] and through the military network defense organizations that are companions with NSA, is unrivaled in their ability to perform a mission under adverse and hostile network conditions. Having said that, we are challenged in theater because of the networks and the diversity of circumstances. And I think that we are facing a generational challenge to overcome this.

I appreciate the suggestion we should have DOD training our allies. The truth is that we have too many cases that we know of of foreign intelligence services likely having penetrated systems that we depend upon for security because they are owned and operated by our friendly host governments, and they may have been designed or built in a way that didn't have first-rate security safeguards. We have seen cases where a national identity system or border control system was having backup tapes of the encounter data sent unencrypted overseas to another country. So it could eas-

ily be penetrated and known, but if known, the tapes, in fact, could be altered.

I don't know if that is typical. That was some time ago. But there are a number of situations like that where basic cyber hygiene and practices that we think of as kind of midlevel protection, not esoteric against high-level threats, just the basics, will not be found overseas, and it is very important that we share that knowledge.

Mr. LANGEVIN. It is disappointing, but a good point to make. Anyone on that point?

If I could then, just my final question to Mr. Costa, what do you see as the future of the Department's human social, cultural and behavioral, or HSCB, monitoring capability after the drawdown of forces in Afghanistan?

Mr. COSTA. Thank you for that question.

I see them as broadly applicable to all the challenges that are facing the Department of Defense, you know, the Intelligence Community and perhaps even State Department. How do we have any sense of short-term instability? How do we predict the next Arab Spring? That is a great goal. We can't predict the next Arab Spring, but how could we predict it? How could we get a sense of awareness of how opinion and behavior and sentiment around the world is changing so that leaders like you and decisionmakers can get a sense a priori of what might be changing? How can we understand how our U.S. messages, whether those are words or deeds, are being received around the world? How can we understand whether our stability actions in country X are having any effect or having our desired effect?

I believe that the technologies associated with what we call this human sociocultural behavior domain have extremely broad applicability, and I have seen them applied to a variety of missions already—countering WMD, countering proliferation, in addition to irregular warfare. So I see the condition quite bright for the applicability of these technologies.

Mr. LANGEVIN. Thank you.

With that I have no further questions. I will yield back and again thank the chairman for holding the hearing, but also to our witnesses for your testimony. Thank you for the work you are doing.

Mr. THORNBERRY. I thank the gentleman.

Mr. Costa, is that sort of modeling more challenging in a tribal society or——

Mr. COSTA. Well, sir, it is always challenging. The modeling is always challenging. And frankly, the more granular you become, the smaller the group you try to model becomes, in some senses it gets more challenging to do it that way. Strategic modeling, while challenging, may be just modeling nation-state interaction.

Mr. THORNBERRY. Yes, yes.

Mr. COSTA. Incredibly complex. But now when we want to go subnationally and model competing groups, we have to have far more data and model to more precision. And in some cases it can be done, but yet the reusability of that model becomes a question. So nations don't change quite that rapidly, but groups can. And so that sort of modeling gets quite complex.

So I think while this technology is very applicable to regular warfare, when we start to move toward subnational and national levels, it gets even more possible and even perhaps more effective.

Mr. THORNBERRY. Interesting.

Let me, if I could, kind of broaden back out to the general topic that we are thinking about today, irregular warfare. My view is that we are going to have a lot more of this in various places all around the world. I think that is inevitable. And I take the point that at least some elements of DOD and other agencies kind of want to turn the page and go back to regular warfare. There is resistance to that.

But I guess I would be interested from each of you as to what sort of capabilities should we look for DOD to retain in thinking about irregular warfare; what sorts of capabilities does it make more sense for DOD to engage the private sector to obtain; and talk about, at least based on your experience, that interaction of DOD choosing to engage the private sector and how well or how poorly that works. So kind of a broader question. Thinking about irregular warfare, what does DOD need to be able to do itself; what can it hire out; and that interaction between the two, oversight, if you will, procurement, where the two come together, how is that going, and how can it be made better?

Mr. ATALLAH. Mr. Chairman, thank you very much for your question.

I guess I would start by saying in order to employ proper IW technologies, I think it is important to define where we want to go, what we want to do. And at times that is not very clear, and therefore it becomes difficult to figure out what type of technologies to use.

So if we take issues like Libya, or Syria today, or Mali, or whatever is going on, first and foremost we have to define what we want the warfighter to achieve at the end, and that is a political process, I think, that would just—at that in terms——

Mr. THORNBERRY. I don't want to interrupt. So you have got to know what your goal is before you can decide what the capability is that you need to have or to procure?

Mr. ATALLAH. Or to procure or invest in.

Mr. THORNBERRY. That has got to be country or case-by-case basis?

Mr. ATALLAH. And so it just depends on what the long-term goals, where our focus is going to be for the up—for the near future. I guess it just boils down to having an end goal in order to—because as I view it, if we are talking about a resource-constrained environment, and we have a shrinking budget, we have to use our resources in an effective way, and therefore we have to pick what we actually invest in.

Technology is great, but I am a former aviator by trade, so we invest in large-ticket items that cost billions of dollars when we can employ less amount of money in technologies that can give us more bang for the buck depending upon where we are going. So that would be one.

I think I mentioned in my testimony when I talk about AFPAK Hands, that is a great program that can be employed, for example, with our regional centers in making our warfighters smarter on

particular regional areas of the world with longevity; meaning that, you know, when we cycle our soldiers out on the battlefield, typically they will have 2 or 3 years in country, and they push out, and then a new person has to relearn the new. But when we have longevity in a particular environment, we become smarter, and therefore we know what technologies to employ based on that environment that we have been living in or operating in for long periods of time. I think that would be the case that I would make.

And so there is no silver bullet for this question, but, you know, the key is defining truly where we want to go in the future. And I would leave it at that.

Mr. THORNBERRY. And I will just comment. I think you are right. Resource-constrained environment, and yet we need to invest ahead of time in the people to have the cultural-social, language capabilities for those places, and that is going to be hard in a resource environment. But your point about the importance of that, the irreplaceability of that when you get into a situation strikes a cord with me, but I think there is going to be that tension. I think you are right about that.

Mr. ATALLAH. Yes, sir. I mean, obviously, again, there is no perfect answer. The enemy is evolving all the time, our issues are evolving all the time. So I think when we go back to basics, and this is probably the point that I am trying to drive home in what I am saying today, is the sociocultural aspect, I think, in everything is extremely important in order to drive where we resource our technologies to be effective in particular problem sets around the world. When I understand the environment, say, for instance, in Lebanon and Syria, and I have spent enough time studying it, I will know what technologies to employ in that particular environment to achieve the end results of what our political process is asking me to do.

Mr. THORNBERRY. Okay. Thank you.

Mr. COHN. Mr. Chairman, I want to be careful how I respond to that. I would like to start, if you don't mind, just by talking for a moment about what it is that I do for a living. My job is to look at commercial technologies and try to figure out where they are cost-effective and applicable to our Government's missions; and likewise, to look at the Government's developed technologies that we are familiar with to see whether they are cost-effective and of value in the private sector. Because my company, three-quarters of our customers are outside the U.S. Federal Government, and that is how we bring value. So we spend a lot of time trying to look at technologies like what I mentioned in my statement earlier regarding personal authentication.

But I would suggest that perfect is the enemy of good, in austere budgets we can't afford to have ambitious, unrealistic stretch objectives driving the way that we build systems and we specify them. I don't think we can afford to have shortfalls and capability where they are vital, but I think it is a very difficult trade-off. And I think we can learn a bit from our commercial programs where there are capabilities that might be good enough and have defense-grade security capabilities built in even if they don't necessarily meet the full list of desired functionality. That may be the best we can afford

in some cases, because the alternative may be providing no capability whatsoever.

And with respect to our current Defense Department and how it handles information technology, I think there is a lot of progress to look at commercial platforms to see how they can apply. The latest Army NIE [Network Integration Evaluation], the integration evaluation, used a commercial smartphone from Samsung as the display unit for maps tied to the Rifleman Radio. That, I think, is an example of what we have no choice of what to do because we can't afford to build ruggedized, military-grade devices that cost 10 times or 100 times as much.

I think the same thing is going to be applied more and more across the spectrum. And my guess is that we will end up with bigger bang for our buck, if you will, but we may also find cases where we have to still deal with specialized development of a custom solution because the military does have unique needs, and balancing that will become the issue.

Mr. THORNBERRY. So you see the trend, because of tight budgets, among other reasons, to using more commercially available technology and making it fit, I guess the "good enough," particularly when we are trying to build partnership capacity.

Mr. COHN. Sir, it is not just because of tight budgets; it is also because of the accelerated pace of change. If you stuck with custom platforms like we used to build to put down the hatches of the nuclear submarines, you would have computers like on the Apollo capsule. If you use commodity IT servers that are coming out that can be configured with virtualization of the cloud, they are so much cheaper, but they are less reliable. If we cluster them together, they work fine.

I think it is also the fact that we want to harness that innovation in the private sector, but we can't do it unless we accept the commercial platforms are modified.

Mr. COSTA. Sir, I would actually start by addressing a point that my colleague to the right just made. I believe that absolutely there is much commercial technology that the Department of Defense and the Federal Government can leverage in the domain that I am speaking to you, in this human terrain domain. There is much technology that can be leveraged, and that is being done. However, there are certainly things that aren't be done by commercial industry, and that has to be done by DOD research. But yet that DOD research needs to transition to the warfighter to programs of record and perhaps back to commercial industry, because that way we both stimulate the economy, and we get that technology into commercial solutions that are then available for the broader Government to bear under challenges.

So I believe that it is both; that we have to leverage commercial technology, but yet the results of DOD research can, in fact, go back into that and stimulate the economy and bring value to the warfighter. But I believe there are low-cost technologies that allow us to understand violent extremists, their networks, their groups, and the spread of their messages, and that is key to irregular warfare. And people on this panel that conduct such analysis can use tools like this to achieve that understanding, at least at some level, while they conduct their deeper understanding.

We also have some technologies that allow us to understand the effects of our messages, and they are still in their infancy. I am not overpromising that any of these technologies are a magic or silver bullet, but they allow us to understand some of the effects. And we are pushing beyond just correlation; we are pushing towards causation: We said the following, and, based on that, this happened, and that was because of our actions. We are pushing toward that. That is a promise, but not yet here.

In addition, we have technologies that allow us to do course-of-action analysis. So if we do X, then Y, we expect the best result to happen. So that also has pertinence to irregular warfare.

So I think with that there are clear things that DOD and the private sector can do. DOD has a clear mission to conduct this irregular warfare. Contractors, companies can help with that in engaging. However, in my domain we can help deeply in helping technology and bringing that to bear on this mission.

Mr. THORNBERRY. And how effective is DOD at figuring out what it needs to invest in itself versus let the private sector do?

Mr. COSTA. Well, personally I have spent a lot of time with the Assistant Secretary of Defense for Research and Engineering staff on the human sociocultural behavior program, and we monitor the commercial environment and work closely with them, so we never willingly, knowingly build something that we could buy. We keep close track of where commercial industry is.

Mr. THORNBERRY. So you think at least in that area it is working pretty well. Keep track of what the commercial sector is doing so you don't duplicate, and then at the same time figure out the key areas where DOD dollars need to be invested.

Mr. COSTA. Absolutely. I believe that we have done a good job in this area. In fact, in this area we are transitioning some of these technologies to commercial companies to, again, close that loop and make those more broadly available. So I do think this is a success story.

Mr. THORNBERRY. I am not sure that is the case in all areas, but I am glad to hear success stories when I can find them.

Mr. Jacobs.

Mr. JACOBS. Thank you again.

Contractors should not collect information. Contractors should not be tasking individuals to collect information. That is an inherently governmental function to collect human intelligence information.

Contractors, on the other hand, can mentor, train, and advise very effectively, and, through observations on the ground, one of the key capabilities of the contractor community is sustainment.

The military has an unbelievable rotation cycle, the OPTEMPO [operational tempo] is just an incredible, difficult thing for our military commanders to manage. They come to Afghanistan for a year and leave. Contractors, on the other hand, have been—I mean from my experience have been on the ground for years in Afghanistan doing the mentoring and training, and developing those key relationships that are required to do this kind of work.

So that is a differentiator between a contractor sustainment over a period of time versus the military.

The other item that I would like to point out to is that the Congress has invested heavily in the past 10 years, since 9/11, in a lot of technologies. Lots and lots of good things have come from that investment. But what my observations have been over time is that we don't institutionalize the success stories, the things that really work, the technologies that really work. And we need to have some resource, some font where that is captured and not lost, and the investment that has been made, hundreds and millions of dollars, will not be lost to the future battles that we will find ourselves in.

We all agree that there are many unsettled states out there, and the technologies that we talk about here will be required. And we know from industry, really through independent assessments and some other tools that we have employed based upon Congress' tasking of those things, we know they work. So we need to capture those things. I don't want that to be lost here today. And——

Mr. THORNBERRY. Capture how?

Mr. JACOBS. We need to capture it in doctrine, in strategy. We need to capture it in schoolhouses by which we teach our leaders; in which we teach, train, and equip our soldiers; we train and equip our State Department foreign specialists, our police advisors. We need to capture these lessons learned, we really do, and it needs to be written down, or it will be lost.

Mr. THORNBERRY. Mr. Franks.

Mr. FRANKS. Thank you, Mr. Chairman, and thank all of you for being here. I know you all contribute in many different ways, many times in your own specific esoteric way, to strengthen the national security of this Nation, and I truly appreciate it.

I am going go ahead and just do a shout-out here. Former Congressman Saxton is in the room here, too. He was here when I came into Congress 11 years ago. And that doesn't mean he is old; that just means he was here. But always grateful to see him.

Mr. Jacobs, if I could, I would like to direct my question to you, sir. Can you share some of the metrics that highlight the successful implementation of these human intel-based programs? You know, I just think that obviously all of us knows the real, best intelligence is boots-on-the-ground, human intelligence, and I would like to get sort of these metrics or the results of some of your human intelligence programs. I mean, how many lives do you think you and your team have been able to actually save, and has that been as a direct result of their sort of unique role in the human terrain? I will follow up if I need to, but it gives you sort of a flavor.

Mr. JACOBS. Sure. Thank you for the question.

There have been great capacity built in the last 4 years on the part of the security forces in Afghanistan both on the police side and on the army side. The results of that mentoring and training has resulted in hundreds of insurgents being captured or killed. I think, you know, probably my last count, over 600 insurgents have been captured or killed. The weapons of insurgency have been taken out of production, in terms of kilograms of the chemicals that are used to hurt and harm and kill our soldiers and marines.

But the more tangential, the more direct is to see the incredible capacity that has been started years ago from a zero now probably to, out of 10, a level five, a level six in terms of their ability to col-

lect information, analyze that information, target and take down the bad guy.

I was in Afghanistan again several weeks ago. There was an attack at the airport. Three years ago that SWAT [Special Weapons and Tactics] capability by the police would have taken days to resolve. This was done in about 4 to 5 hours. They came, they identified, they secured the perimeter to protect the public, and killed the bad guys. Pretty impressive. Pretty impressive. That is progress. That really is tangential progress on the ground.

And so I don't want to get into a lot of specifics, but one of the beauties that I think every successful program needs to have an independent analysis by a third party to look at it and to kick the tires. It is very important. And the RAND Corporation has done that on our Legacy program, funded by the United States Congress, to look at whether or not this truly is a unique capability that we should have. And the studies have begun in 2008, and they go on to this day. Legacy is probably one of the most unique programs that have been countless studied by RAND, and without a doubt they show clearly that these kinds of programs work, and that we should have this capability in our arsenal, in our toolbox of irregular warfare.

The other thing that the RAND Corporation has talked about is the measures of effectiveness that we go into, and we measure—we have 500 data points, and I am not going to get into all the details of that, but those data points measure—are quantifiable and measurable to the outcomes of the program. And it ensures that the taxpayers are getting their money's worth, that this program actually works. And that is why we do what we do.

So I know I have been rambling a little bit and covered a lot of things, but——

Mr. FRANKS. Mr. Chairman, if you would afford me just one last followup here, because I have been listening very carefully to what you are saying, and I am wondering if you might have—because I know it is impossible to get into some of the minutiae, but if you might have some sort of compilation of some of the things that we are talking about here today, and, as you know, especially that you could give us to that would have an impact not only to the members of this committee, but to the larger membership of the Armed Services Committee.

And as we move forward, it seems especially important with this transition period in Afghanistan where combat operations will soon draw to a close, would you say programs like this will increase or decrease in importance? And what are some of the hardware tools that best suit operators who are trying to build intelligence capacity in this environment? You know, it especially seems like a relevant question given that some of the majority of our Afghan partners are still using technology like flip cell phones.

Mr. JACOBS. That is right. That is right.

Mr. FRANKS. I would love to get some sort of written overview of this, because if this is saving lives, and you are saying—your testimony is that this is saving lives——

[The information referred to can be found in the Appendix on page 79.]

Mr. JACOBS. It is saving lives.

Mr. FRANKS [continuing]. Of American and coalition lives.

Mr. JACOBS. Yes, yes.

One thing I would caution. A lot of things get caught up in drawdowns, you know, and we need to be very careful not to cut the ability to build capacity by our allies. And my concern is that in the rush we don't leave a true capacity on the part of our Afghan partners to penetrate networks. And that needs to be sustained, mentored, and continued to be nurtured on the part of the United States of America.

Mr. FRANKS. Thank you, Mr. Chairman.

Mr. THORNBERRY. Mr. Atallah, we have got security challenges all across Africa. Would you foresee that it would make sense for the Government to hire companies to help build capacity, improve security forces in some of the various countries you are familiar with?

Mr. ATALLAH. Mr. Chairman, thank you very much for your question.

Certainly companies can provide capabilities, absolutely. I think these companies need to be carefully selected. I think we need to also carefully select what we employ, because as we make certain countries more capable, we also—at the same time the enemy becomes more capable in time, adjusting to, you know, what the realities are on the ground. And so we got to define that and figure out what we are trying to achieve; again going back to my earlier statement is what is our end game? Once we define that, we can obviously employ—there are places across the Sahel; of course, in Somalia now, we are looking at tensions between, you know, the two Sudans, and Egypt and Ethiopia. These are going to continue to fester. And there are certainly places with our small companies like we see here, or mine, where we can bring in some of that; we can bridge the gap between usage of proper, well-fitted technologies into specific cultures to achieve the end means that we are aiming for.

And I always go back to the problem is not what we are capable; we can do a lot of stuff. The thing is, are we doing the right things? That is the question is what does right look like at the end? And I think that is important to actually answer.

Mr. THORNBERRY. Great.

Well, thank you all. I appreciate it. I think this is going to be a topic that occupies us a lot in the years to come, and each of you have helped enlighten me at least on how to move forward. So again, thank you for being here, thank you for your testimony, and thank you for your patience on our interruption. With that the hearing stands adjourned.

[Whereupon, at 12:23 p.m., the subcommittee was adjourned.]

APPENDIX

JUNE 28, 2013

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JUNE 28, 2013

Prepared Statement of

Rudolph Atallah (Lt Col USAF, ret.)
Chief Executive Officer
White Mountain Research
and
Senior Fellow, Michael S. Ansari Africa Center,
Atlantic Council

And

Jeffrey B. Cozzens
President
White Mountain Research
and
Fellow, Center for Infrastructure Protection and Homeland Security,
George Mason University

Before the

United States House of Representatives
Committee on Armed Services
Subcommittee on Intelligence, Emerging Threats and Capabilities

On

"Past, Present, and Future Irregular Warfare Challenges:
Private Sector Perspectives"

Friday, 28 June 2013
10:00 a.m.
Rayburn House Office Building, Room 2118
Washington, D.C.

Introduction
Mr. Chairman and Honorable Members of the Subcommittee:

Thank you very much for inviting me to testify today on the irregular warfare challenges that my colleague, Jeffrey Cozzens, and I have observed since 2001. My testimony focuses on framing some of principal IW challenges that have crystallized since 2001—problems that will continue to demand persistence, unconventional thinking and the full commitment of our defense and intelligence communities to address. I will close with some thoughts concerning the maintenance and improvement of our national IW proficiencies as we seek to meet future challenges.

Our written response to the Committee's queries and my testimony today is rooted in my experience as an Africanist and former special operations and OSD policy professional, and Mr. Cozzens' background as a terrorism researcher and alternative assessments specialist. We have both been involved with the conceptualization and planning of IW activities in Africa, the Middle East and elsewhere, and continue to advise the US Government on matters of cultural intelligence, counter-terrorism and other activities germane to IW through our small business, White Mountain Research.

About White Mountain Research LLC
White Mountain Research (WMR) is a Virginia-based small business providing tailored international security solutions to U.S. Government and commercial clients. Jeffrey Cozzens and I lead WMR, supported by an international contingent of former special operations professionals, terrorism subject matter experts and some of the world's foremost Africa analysts. We deliver maximum value to our clients by fusing practical operational know-how, creative approaches to cultural and human intelligence and global interdisciplinary academic expertise.

Before I begin, let me say that we recognize that technology plays an important role in IW; however, we believe it is *subordinate* in importance to IW's human ways and means. My testimony therefore highlights the imperative of understanding the humanity, thought and behavior of our non-Western allies and adversaries while emphasizing the centrality of human intelligence (HUMINT) in IW. Eroding irregular adversaries' ideological and social centers of gravity and wielding the influence required to win at war's moral level—critical in an age where social media turns tactical missteps into strategic conundrums—can only be achieved through the access, dexterity and context afforded by properly equipped warriors and analysts. Technology, while it can assist in this process, cannot take their place.

Definitions
For our purposes, irregular warfare (IW) can be defined as warfare that involves one or more irregular forces—especially non-state actors—and favors asymmetric and indirect approaches designed to win legitimacy and influence while eroding an adversary's. Some of the more common contemporary manifestations of IW include terrorism and counter-terrorism (CT), forms of transnational criminality, insurgency and counter-insurgency (COIN), foreign internal defense (FID) and so forth.

IW challenges and lessons-learned since 2001

Allow me to outline some of the challenges and lessons-learned of the past 12 years that we find most striking:

Challenge 1: Understanding non-Western friends and foes

Perhaps the greatest challenge to IW observed since the 9/11 attacks is our inability to accurately understand and therefore project how and why non-state allies and adversaries—including those inspired by militant strands of political Islam—think, organize and operate. Part of this problem set arises from of our institutional tendency towards mirror-imaging—that is, thinking like professional soldiers, analysts and policy-makers rather than non-Western activists, bureaucrats or militants, motivated as much by identity, belief or cultural imperatives as they are by traditional notions of strategy. Our struggles in this respect are related to or have birthed a subset of challenges, each of which deserves more attention than this paper can afford. These include:

- The obvious but monumental complexities associated with combatting virulent ideologies that are associated with a major monotheistic religion or are an offshoot of a legitimate social movement.[1] Challenging extremist ideologies across changing national boundaries, socio-cultural contexts and legal environments naturally adds to the density and scope of the problem.
- Consistently and accurately understanding adversaries'—or for that matter, partner states' or tribes'—victory metrics[2], negotiating strategies and decision-making.
- Turning allies into enemies because our planning has, in some instances, not thoroughly and accurately accounted for the strategic impact of tactical errors that have offended codes of faith, honor and dignity. Globalized technologies like social media instantaneously amplify these errors and feed the recruitment narratives of irregular foes, which thrive like parasites on perceived victimization and perceptions of American hypocrisy.

Challenge 2: Overreliance on technology

Despite recognition since 9/11 of the importance of socio-cultural understanding, the reality of our approach to IW remains focused on 'zeroes' and 'ones'; we continue to rely increasingly on intelligence derived from technical sources and less on HUMINT. Context derived from understanding and thinking like 'others' takes a backseat to information. Beyond the monetary burden associated with overreliance on war-fighting technologies, our ability to grasp and contend with complex socio-cultural issues is gradually eroded. The cost beyond billions of dollars is misunderstanding (or missing altogether) important underlying factors of conflict, potential alliances and opportunities to pursue long-term, effective direct

[1] See Jeffrey B. Cozzens, "The Culture of Global Jihad: Character, Future Challenges and Recommendations," *Future Actions Series*, International Centre for the Study of Radicalization, King's College London (April 2009).

[2] Jeffrey B. Cozzens, "Victory—From the Prism of Jihadi Culture," *Joint Force Quarterly* (January 2009).

and indirect solutions to irregular challenges. The role of the MNLA in Mali is, in our view, a case in point.[3]

Further, since the first Gulf War, we have developed high-tech solutions that lend warfighters the ability to quickly find, fix and finish enemy targets. Our soldiers have grown accustomed to possessing enormous amounts of intelligence data at their fingertips that provide answers to almost every question arising within the operating environment. But whether the financial resources required to sustain this technology will be there in the coming lean years is unknown. If the economists are correct, SOF units will have to return to more traditional modes of working as small units conducting operations "by, with and through" local military liaison forces and other local surrogates and, in extremis, as independent units working from commander's intent with little support from either US or friendly local forces. Although advanced technologies will certainly play a role in these cases, these small units will succeed or fail based on their ability to analyze, fight and navigate within the local environment. Their ability to understand cultural context is essential to finding victory in such limited operations. The question is whether we are doing enough institutionally to prepare them.

Challenge 3: Defining the political outcomes of IW
It is a well-known maxim that war is 'politics by other means'. Agreeing here with Clausewitz, a clear understanding of our objectives and strategies in waging IW is essential, especially given the primacy of influence and winning at war's moral level. Further, the clear articulation of these objectives—basically, our desired 'end-state'—to the American public is also key, given the necessity to generate Americans' support for the long-term operations and patience that characterize effective irregular warfare. Without a clear articulation of our desired ends, how can we measure effective means? We do not believe that this question has been asked enough in the halls of the Pentagon since 2001. Irregular warfare has often appeared as an end in itself.

Challenge 4: Limited SME immersion
Another apparent challenge in combatting irregular and geographically dispersed threats is a lack of reliable subject matter expertise. Generating a meaningful understanding of a country or region's socio-cultural issues requires years of immersion. It has been our observation that, when DoD reacts to a new issue, it often reaches out to academia for answers. However, it is often the case that academic advisors have limited understanding of ground-truth socio-cultural context because their 'expertise' is gleaned from desktop research or a couple trips to a distant capital. Instead of turning to individuals who have spent meaningful time on the ground conducting fieldwork and developing objective qualitative

[3] Rudolph Atallah, testimony on security in the Sahel and West Africa before the US House of Representatives, Committee on Foreign Affairs (21 May 2013), at: http://docs.house.gov/meetings/FA/FA16/20130521/100886/HHRG-113-FA16-Wstate-AtallahR-20130521.pdf

perspectives on the challenges at hand, DoD too often invests in shallow and often biased 'expert' opinions. The result is a poor, often skewed understanding of both the problem-set and the environment that is nevertheless translated into IW planning.

Of course, another principal secondary challenge within the problem of expertise is one of scope and timeliness—scope because IW problem-sets evolve and disperse so quickly, and time because the bureaucratic and vetting mechanisms required to find and place credentialed experts (or develop them from within DoD) produce huge opportunity costs. Again we turn to the crisis in Mali for an example.

Challenge 5: Negating the advantages of suicide operations
Suicide tactics—whether through an improvised explosives device, a small unit like the Mumbai attackers, or an individual gunmen—and the innovation and commitment that drives their effectiveness are some of the primary operational challenges of our age. In crafting effective IW, negating the operational, cultural, and even spiritual advantages of suicide bombing must remain a consideration, as this method will continue to remain a preferred weapon of mass effect for irregular combatants.

Many of the advantages of suicide bombing operations are well know, but merit listing here to showcase the human element:

- The function of the suicide bomber as a 'smart bomb', who operates flexibly at both a strategic and tactical level to hit targets of mass effect commensurate with the 'intent' of his movement or commander.
- The demonstrative element of suicide bombing, enflamed by the prominent media (and social media) coverage it receives, aiding not only in publicizing a terrorist's cause but also in 'striking fear'—a primary objective.
- The ability of suicide operatives to dismiss the traditional pillars of Western Cold War strategic theory: deterrence, pre-emption and early warning.
- The attractiveness of martyrdom as a reward for the operative and his/her cause, whether politically, social and/or religious in nature, which compels the operative(s) to complete their mission;
- The attractiveness of the act as an end in itself for some militants.
- The fact that suicide operatives waste little time deliberating about how to evade authorities after an attack or face interrogators; and
- The low cost and technical simplicity of most suicide IEDs and operations.

Challenge 6: Improvised explosive devices (IEDs)
Finally—and related to the above point on suicide tactics—is the challenge posed by IEDs and their continued use and improvement. From Afghanistan, to Iraq, to Boston, the IED remains a weapon of choice for the weak owing to its simplicity to construct, its globalized and highly replicable nature and its potential to generate surprise, mass casualties and strategic impact. Terrorists and insurgents are continually upgrading or even simplifying their designs in a bid to overcome our

sophisticated and costly defenses. They still too often succeed. While a host of DoD entities have made tremendous progress in IED detection, defeat and various other counter-measures, the threat persists and will continue into the foreseeable future.

Recommendations

The last 12 years have been defined by an evolving spectrum of irregular threats and asymmetric methods. Much of our global contest with movements like al-Qaeda and its transnational contemporaries have been waged in unfamiliar and high-context areas that test not only our financial wherewithal but also our human capital. In agreement with most on this panel, we believe this pattern will continue.

On this point, we offer several parting thoughts for improvement as we look to the next 12 years of IW:

First, we need to expand our HUMINT capabilities. As American war-fighters, we will always have the ability to do 'something', but having good intelligence coupled with solid context allows us to do the right thing.

Second, we need to couple an expanded HUMINT capability with new methods of socio-cultural training and alternative analysis programs that promote viewing the environment through the eyes of non-Westerners. Years ago, the Air Force began a new career path for its officers in which they were required to focus on a region with an aim to learn the culture and an associated language. The goal was to groom officers with socio-cultural skills and knowledge so they can become more effective diplomat-warriors in the future. This program exemplified the forward thinking that needs to be encouraged as we prepare for future IW. The Marine Corps and Army have offered many similar programs, although some like the Army Directed Studies Office have, unfortunately, fallen by the wayside just when they are needed most.

Third, **continued private sector partnerships are essential for DoD. Businesses like White Mountain Research that work overseas have a great deal to offer, as the market forces us to stay in-tune with foreign political and socio-cultural issues in order to compete.** As we conduct our peer-to-peer research and keep pace with local politics in foreign countries, DoD can gain richly from our experiences.

Fourth, interagency best practices for planning kinetic operations should also be used in non-kinetic planning. We know how to work together to identify and pursue targets. However, we do not typically follow the same principles and patterns when dealing with non-kinetic challenges.

Fifth, we must bear in mind that everything has an economic limitation. Based on this, at the political level, we should determine what we want our objectives to look like and define and calibrate appropriate IW resources to meet it. At the grand

strategic level, we must also recall that national culture is a powerful instrument that could be leveraged more effectively than it has.

Sixth, IEDs have been around from the inception of gunpowder. We should keep organizations like JEIDDO open because this problem will never go away. The Boston bombing is a case in point. Our ability to minimize, defeat, prevent IED attacks is an important part of our IW capability.

Seventh, the lack of continuity in DoD must be addressed. Most soldiers never exceed more than two or three years in an overseas country assignment. Unfortunately, with each rotation, their replacement has to learn local issues from the start, even when the institutional knowledge is there. This does not allow for the sustained familiarity with the host country that is so crucial in IW. To be more effective, DoD should allow a soldier to focus on a region (a group of countries sharing a common border) for a minimum of five years and include a yearlong overlap with the inbound soldier. This will provide the opportunity to develop meaningful local networks more quickly and transition critical knowledge. This is why programs like AFPAK Hands[4] must be continued and expanded to other regions of the world. These programs can dovetail well with regional centers of excellence like the Africa Center for Strategic Studies (ACSS) or the George C. Marshall Center.

Eighth, in combat zones, soldiers are too often restricted to secure locations, negating important opportunities for cultural immersion. This has the potential to taint soldiers' perspectives and can create an "us versus them" mentality with strategic consequences. We know that effectiveness typically increases for Special Operators who dismount vehicles and engage with the local populations. Most will tell you that they garner important cultural signals this way, making them vastly more efficient and empowered war-fighters. Their lessons-learned should be applied in a wide swathe across DoD.

Finally, more effective and systematic screening procedures should be instituted for academic advisors. These should be vetted for not only their subject matter knowledge, but also their objectivity. When advising on far-flung places like Mali or Nigeria, extensive on the ground experience should also be a prerequisite before they are put in a position to educate our warfighters. We have witnessed too many times the unfortunate consequences of unprepared and/or biased advisors hired to provide direction to crucial DoD initiatives.

[4] See http://www.jcs.mil/page.aspx?id=52

RUDOLPH ATALLAH

COUNTERTERRORISM & POLITICAL/MILITARY SPECIALIST

Air Force Lt Colonel Retired • Foreign Area Officer – Africa/Middle East/Europe • Linguist (French/Arabic)

Counterterrorism strategist specializing in political & military negotiations at the highest levels of leadership. Designed approaches for East, North & Sahel regions of Africa. Accredited Air Force Defense Attaché to 6 African countries; possess extensive *on-the-ground* experience across the continent. Requested by name to speak at numerous government, military, academic, & civilian conferences / symposiums. Able to represent policy to Congress & Senate. A 17-year Middle East resident who has traveled to100+ countries & met w/5 heads of state.

EXPERIENCE

Chief Executive Officer (CEO) 12/2009 to Present

White Mountain Research LLC (WMR), Herndon, Virginia

WMR is a service disabled veteran owned small business that is dedicated to understanding and mitigating complex threats to human security. Built the company from the bottom up, from 2009-2011, WMR grew by 400% taking on contracts with US government agencies and corporate clients.

- Led & negotiated 5 successful hostage releases from Somali pirates.
- Planned/developed emergency evacuation plans from Egypt for DODI, a Houston based Oil Company. Worked w/senior executives on crisis planning to protect 3 oil rigs. Saved $3 million/day.
- Led event security for 3 of ICANN's (Internet Corporation for Assigned Names & Numbers) 1200 person conferences in Kenya, Columbia & Senegal – 100% success.
- Taught risk management class to 430+ oil workers in Norway, Egypt & UAE. Reduced mishaps by 50%.

Africa Counterterrorism (CT) Director / Morocco-Tunisia Country Director 4/2007 to 9/2009

Office of the Secretary of Defense (OSD), Pentagon, Washington, DC

Only Foreign Area Officer in the Air Force concurrently holding three regional specialization designations – Africa, Middle East, and Europe. Informed and advised the Secretary of Defense (SecDef) on CT policy & strategy in Africa and related engagement with Morocco and Tunisia. Orchestrated conferences with Ministry of Defense (MOD) officials of Morocco and Tunisia. Developed strategic CT initiatives, programs & activities to enhance U.S. national security interests through evaluation of regional political & military developments. Supervised security cooperation, military training & humanitarian assistance programming. Advocated CT policy w/United Nations.

- Briefed Congress and Senate on counterterrorism activities/operations against violent extremists in Somalia.
- Worked in the office of the Secretary over the last 6 years on complex political/military issues ranging from CT operations to complex border disputes (Ethiopia/Eritrea) and mil to mil engagements.
- Led first ever OSD Policy U.S./European Africa CT conference, resulting in new policy changes designed to reduce terrorist threats from Africa. Also increased terrorist captures through new strategy development.
- OSD's point-man for Morocco's $2.1 billion purchase of F-16 and T-6 aircraft from U.S. manufacturers.
- Instrumental in steering Morocco's choice of aircraft over French jet fighter by using effective negotiation.
- Advised DoD Senior official during visit to Djibouti, Ethiopia & France to discuss the establishment of Africa Command (AFRICOM).
- Worked w/SOCOM on the rescue of Capt Philips (MAERSK ALABAMA) from pirates off the Somali coast. Provided key information/strategy, which led to his rescue.

Africa Counterterrorism Director / East Africa Director 6/2003 to 4/2007

Office of the Secretary Of Defense, Pentagon, Washington, DC

Informed & advised SecDef on CT policy and strategy in Africa and related engagement with nations in the Horn of Africa (HOA). Supervised security cooperation, military training & humanitarian assistance programming. Advocated CT policy among foreign governments, the UN, Congress and interagency intelligence organizations. Developed strategic CT initiatives, programs, activities & intelligence policies to enhance U.S. national security interests through evaluation of regional political & military developments. Handpicked to be key advisor for the Air Force on Defense Attaché panels.

- Led/negotiated w/Government of Djibouti the expansion of 1st forward-operating base in Africa. (10-year, $1.5 billion deal)
- Lead strategist in crafting Somali policy to eliminate Al Qaeda activity & protect U.S. interest in the HOA.
- Outlined innovative approach to counter piracy off the Somali coast, lessening food crisis affecting more than 14 million people in the horn of Africa.

- Led DoD team to advance counterterrorism plans with Kenya, Djibouti and Ethiopia.
- Invited by SOCOM & UAE's crowned Prince as guest speaker to the CT Symposium in Abu Dhabi.
- Spearheaded initiative leading to the capture of 10 pirates and rescue of an Indian vessel with 16 hostages off Somali coast through development and implementation of a counter-piracy policy.

Air Force Defense Attaché 6/2000 to 6/2003
Defense Intelligence Agency, United States Embassy – Abidjan, Cote d'Ivoire
Represented the Sec/Air Force & Commander of U.S. Air Force Europe. Advised U.S. Ambassadors in 6 West African nations, their respective national air forces and MODs on Air Force matters. Reported on military & political matters leading to formulation of U.S. policy supporting regional national security interests, crisis contingency planning & response. Directed air operations for C-12 aircraft supporting U.S. diplomatic missions & defense attaches in 24 African countries.

- Led most active C-12 aircraft program in the Defense Attaché system.
- Judged most effective Air Force liaison to military leaders in 6 nations due to knowledge of the region and fluency in both French and Arabic.
- Authored 1/3 of intelligence reports in the Defense Attaché's Office.
- Assisted evacuation of 1,700+ American Citizens from Ivory Coast following 2002 coup.
- Spent extensive time on the ground in West / Central Africa seeking out extremist in response to 9-11.
- Sought by key embassy officials for insight on local Arabic-speaking communities.

Director / Instructor - Sub-Saharan Orientation Course 6/1997 to 6/2000
Joint Special Operations University, Hurlburt Field, FL
Directed/managed the Sub-Saharan Africa Orientation Course, instructing military & government civilian personnel on political, military, economic, and cultural aspects of Sub-Saharan region. Taught officer courses to CT & Special Operations Forces staff. Developed new coursework utilized in Middle East & CT programs.

- Handpicked by OSD to instruct in first-ever senior African civil-military course in Senegal, West Africa.
- Extraordinary instructor teaching 5 separate courses relevant to regional terrorism and security issues.
- Only AF pilot to advise 3rd Special Forces Group on integration of airlift into Africa peacekeeping program.

ADDITIONAL EXPERIENCE

Senior Fellow at ANSARI African Center
Wing Flight Safety Officer / C-141 Aircraft Commander
United States Air Force - 60th Air Mobility Wing, Travis Air Force Base, CA
Directed and supervised 35 base safety programs ensuring flight and aircraft safety.
Over 4,000 flight hours to include combat flight time.

EDUCATION & TRAINING

Masters of Science, International Relations, Troy University, AL
Bachelor of Science, Electrical & Biomedical Engineering, University of Connecticut, Storrs, CT
Squadron Officer School & Air Command and Staff College
Joint Military Attaché School
Multiple C-141 / C-12 Qualification, Instructor Pilot and Aircraft Commander Schools
Air Force Flight Safety School, Top Graduate
Dynamics of International Terrorism; African Studies

CERTIFICATIONS

- Fixed Wing Multi-engine Instructor Pilot / Multi-engine and Instrument Rated Pilot / Air Refueling Pilot
- PADI Advanced Open Water Diver

AWARDS/ACHIEVEMENTS
Over 25 military honors *including:* Defense Meritorious Service Medal for direct involvement in the rescue of Capt Philips and 6 years of OSD Policy achievements.

DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 113th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee.

Witness name: **Rudolph Atallah**

Capacity in which appearing: (check one)

___Individual

__X_Representative

If appearing in a representative capacity, name of the company, association or other entity being represented:

FISCAL YEAR 2013

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Contract	DoD	$65,000	Mapping Mali's elections

FISCAL YEAR 2012

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Contract	DoD	$93,161.35	CT Knowledge/CT support
Contract	DoD	$95,000.00	De-radicalization Support

FISCAL YEAR 2011

Federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Contract	DoD	$406,622.00	EU counter-rad & CT

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2013):_____1_____;
Fiscal year 2012:_____2_____;
Fiscal year 2011:_____1_____.

Federal agencies with which federal contracts are held:

Current fiscal year (2013):_____DoD_____;
Fiscal year 2012:_____DoD_____;
Fiscal year 2011:_____DoD_____.

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

Aggregate dollar value of federal contracts held:

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

Federal agencies with which federal grants are held:

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

Aggregate dollar value of federal grants held:

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

Past, Present, and Future Irregular Warfare Challenges: Private Sector Perspectives

Statement of Mr. Mark L. Cohn
Vice President, Engineering and Chief Technology Officer
Unisys Federal Systems, Unisys Corporation

Before the
House Armed Services Committee
Subcommittee on Intelligence,
Emerging Threats and Capabilities

June 28, 2013

Good morning Chairman Thornberry, Ranking Member Langevin, and other distinguished Members of the Subcommittee. I am Mark Cohn, Vice President Engineering and Chief Technology Officer for Federal Systems at Unisys Corporation. We thank you for inviting Unisys to participate in this hearing focusing on lessons learned in irregular warfare, challenges that remain in today's operating environments, and how industry can contribute to enhancing our security.

Unisys is a global corporation, headquartered in Blue Bell, Pennsylvania with 22,000 employees in over 100 countries providing information systems solutions and services to a wide range of private and public sector customers. Unisys has a long and proud history of serving our federal government. We provide solutions for 1500 government entities around the world.

Around the world and here at home, Unisys is a leading provider of integrated security solutions – many of which incorporate advanced biometric and identity management technologies. For example, we delivered a national identification card for Malaysia that employs fingerprint identification and supports real-time biometric verification of identity at traffic stops and biometrically-protected automated border control. We delivered a national identification system for Angola with multiple biometrics that required mobile enrollment in the villages under austere conditions. It provides counterfeit-resistant proof of identity to a large and widely dispersed population, as a cornerstone of citizenship in an emerging democracy to support proof of the right to vote and for future access to multiple government services. Recently, we delivered a system for Mexico that provides for storage of 110 million identification records comprising fingerprints, facial images, and iris scans with the capacity to process 250,000 new enrollments daily. Enrollments are underway starting with youth and extending to Mexico's entire adult population. Mexico's Secretary of Government (SEGOB) stated that the use of iris recognition, along with other biometric data, serves to combat crime such as human trafficking and to streamline registration and enrollment procedures in schools and health care programs. These systems, along with those we furnish to national security and law enforcement organizations, provide reliable technology to verify the identities of known individuals and the means to identify unknown individuals.

To defend the nation and defeat our adversaries engaged in irregular warfare, the Department of Defense requires capabilities in counterterrorism, counterinsurgency, foreign internal defense, and stability operations. Our military operates with other U.S. governmental agencies, multinational partners, and the partner nation to develop plans for coordinated action and to minimize the reliance on U.S. military and security presence. In the long run, it is ultimately a political contest for legitimacy and influence over a relevant portion of the population that depends on a capable local partner to address the conflict's causes and provide security, good governance, and economic development. However, counterinsurgency operations depend on separating enemy combatants from innocent civilians in the general population.

Generally state and/or non-state actors resort to irregular warfare when traditional methods of warfare are not ideally suited to reach their objectives or they do not have the resources to fight against a stronger adversary. In irregular warfare, a primary U.S. objective is to create a safe, secure environment for friendly populations and friendly military forces and to mitigate disruptions to their daily lives. This can help to grow or maintain popular support for the government or entity the U.S. is supporting. Providing a safe environment is complex during irregular warfare as the "enemy" generally is well concealed within the population. The "enemy" can involve a number of non-state actors, such as terrorists, criminal enterprises and warlord militias, that are difficult to identify among the general population, and this enhances their ability to carry out surprise attacks on the population. Another challenge in irregular warfare is being able to distinguish loyal indigenous security forces from disloyal foes who can procure uniforms and equipment that allow them to blend with regular forces and conduct surprise attacks on installations or within government buildings that could have strategic policy implications.

Biometrics, the application of technology and science to measure physical characteristics to determine the identity of individuals, can play a valuable role in irregular warfare by helping to prevent and disrupt irregular threats by identifying targets of interest, deny movement to adversaries, and protect civilians and military forces. It is important to recognize there are limitations to biometric systems and methods as data captured for these purposes by U.S. personnel generally requires close physical proximity to the subject, usually is episodic and selective because cooperative participation by subjects cannot be expected, and relies upon

equipment and a system architecture that reportedly fails at times to fully address operational needs. Today's tactical collection equipment employs custom-built integrated mobile kits that can be bulky and cumbersome and reportedly there are issues with data synchronization and other factors limiting effective tactical use (referring to GAO report GAO-12-442, pages 16-24). Industry can help by taking advantage of new mobile processing platforms derived from consumer mobile devices configured for rugged conditions and extended with biometric sensors and by implementing interfaces in a unified architecture that streamlines information interchange from tactical collection to an authoritative database so that submissions are received and match/no-match results are provided to operators consistently and quickly. It is essential that transmitted and stored identity information and biometrics stay coupled because separation of the data undermines the system's speed, accuracy and ability to detect enemy combatants. With respect to facility security and force protection, more advanced biometric techniques than are in use today are possible to improve verification of identity for U.S. and coalition military personnel and civilian partners and without requiring the person undergoing verification close proximity to friendly forces. One example is three-dimensional facial recognition which does not depend on the use of visible light so it can operate at night without calling attention to itself. At facilities and checkpoints, this would allow greater stand-off distances reducing the threats posed by suicide bombers. Another example is improved 2-dimensional and what is called "2.5 dimensional" facial recognition algorithm performance, intelligent camera systems, and face detection analytics that could enable capture of unobtrusive non-cooperative biometric data to identify and associate individuals observed at improvised explosive device detection sites.

Unisys longstanding experience providing integrated biometric credentialing solutions in countries such as Malaysia, Australia, Canada, South Africa, Chile, Costa Rica and Spain indicates that other countries are using wide-scale identity management and biometrics to protect borders, secure transportation facilities, and to improve the efficiency of the administration for public services. Some focus on electoral participation or on delivery of social services. The relative cost and performance of such systems has improved dramatically in the last twelve to fifteen years with greater reliance today on multiple biometrics simultaneously captured for enrollment (not just two fingerprints for example but capturing all ten and adding facial and/or iris), proven large scale adoption of commercial frameworks that reduce development time and

risk, and emergence of standards and services based architectures that enable vendor independence in selecting algorithms and building systems that can evolve. The biometric systems that Unisys deployed in Angola and Mexico can be seen as examples where these trends have come together. Both were implemented rapidly at predictable cost because we used a framework of proven components to enable the various delivered systems to be flexible, scalable, secure, and to utilize multiple workflows and biometric modalities independent of the algorithm vendors, and to rely on standards-compliant open interfaces.

There has been a great expansion in the number of economically viable use cases for biometrics to support access control such as neighborhood policing (badging systems for use at checkpoints to achieve local area security), protecting access to government buildings and military installations, humanitarian assistance identification systems to reduce fraud in distribution of aid, and international border control systems to improve security. For instance, we implemented a system that the Port of Halifax that uses vascular biometrics for access to the port by 5,000 workers and the Restricted Area Identity Card with fingerprint and iris for access to Canada's 28 major airports. DNA matching is now more widely used in forensic identification systems to combat crime and also increasingly for purposes such as kinship analysis for disaster victim identification. In all regions of the world, we see widespread user acceptance of biometrics for secure access to sensitive facilities including international borders and for consumer convenience such as protecting electronic banking records and securing air travel. Consumer mobile applications will increasingly rely on biometrics captured with inexpensive sensors (for voice, face, and touch). There is significant commercial interest in banking and other regulated industries because anti-spoofing techniques can easily be employed and biometrics can simplify the user experience while increasing security when compared with password or personal identification number (PIN). This could provide advantages for some purposes over today's Department of Defense personnel authentication approach that relies on Common Access Card (CAC) and PIN. A commercially available biometrics-driven alternative used today in the banking sector would be more convenient, less expensive and time consuming to administer, would eliminate the problem of transport and lockout during PIN reset, and could address risks such as the impostor threat that the current CAC and PIN model cannot. Low cost and deployment "footprint" mean this could be used to secure access by non-government

organizations and partner country personnel to electronic systems for sharing situational awareness information.

We believe the Department of Defense can expect that these international and industry developments are in many cases applicable to the challenges we face when confronting adversaries in irregular warfare and in improving the internal security and stability of the societies that we are working to stabilize both through U.S. and partner country initiatives. Unisys looks forward to supporting that progress both here and overseas.

Mark L. Cohn
Vice President Engineering
Chief Technology Officer, Federal Systems
Unisys Corporation

Mark Cohn is vice president engineering and chief technology officer for Unisys Federal Systems. He directs portfolio strategy and solution development for major Federal Systems programs to bring innovation to the marketplace and expand the mission impact of IT. He is organizing Unisys capabilities that enable mobility, analytics, and cloud-driven enterprise transformation and acts as technology emissary for Unisys with industry partners and enterprise customers.

Prior to his current assignment, Mark served as partner and vice president, Enterprise Security for Unisys with responsibility for the vision and management of security solutions and services programs across the company while managing the Federal Systems Enterprise Security practice. He was a principal spokesperson and leader of the Unisys global team of experts in the application of information technology to physical security and surveillance systems, transportation, and international border security and was the Unisys representative for government-industry liaison on cybersecurity and critical infrastructure protection.

Since joining Unisys in 1985, Mark has served successfully in a broad range of engineering and management positions. For several years, Mark was vice president and chief architect for Unisys Global Public Sector, where he provided technical leadership for public sector engagements in defense and domestic security. As chief engineer and technical services director for border security and critical infrastructure, he managed mission system engineering and product development for the first phase Common Operational Picture system. He was technical advisor and executive of interest for Unisys with the DoD Counterintelligence Field Activity, program manager for the Transportation Security Administration Registered Traveler pilot program and principal architect for the Department of Homeland Security US-VISIT Exit system. Prior to that, he managed the transition to Unisys of IT Production Support at the Executive Office of the President and architected the technical solution for the TSA Information Technology Managed Services contract, as well as several interagency law enforcement information sharing systems.

In 2001, Mark was chief architect for modernizing Unisys health care solutions to move from mainframe to Wintel servers and comply with HIPAA regulations. From 1997 through 2000, he was general manager of the architecture and software development practice of Federal Systems, where he directed Unisys e-government initiatives and managed a $25 million per year portfolio of programs from sales through service delivery at the Departments of Education, HHS, HUD, and Transportation and at the FAA, Military Health Service, National Guard Bureau and GSA Public Buildings Service.

Mark is an expert in the design and implementation of trustworthy, highly available distributed systems. He began his career at Unisys as a senior systems programmer on fault-tolerant systems used for aviation infrastructure management and was the principal designer and chief engineer for nationwide critical command and control capabilities essential to air traffic control that have proven to be among the most reliable systems ever put into operation.

Mark was educated at MIT and the University of Maryland with a bachelor's degree in behavioral and social sciences. He has a graduate certificate in management information systems and a master's degree in management of technology from American University. He was a Certified Computer Programmer and is currently a Certified Information Security Manager and Project Management Professional. He resides in Washington DC.

DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION

Instruction to Witnesses: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 113th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number will be made publicly available in electronic form not later than one day after the witness's appearance before the committee.

Witness name: Mr. Mark L. Cohn

Capacity in which appearing: (check one)

__ Individual

X Representative

If appearing in a representative capacity, name of company, association or other entity being represented: Unisys Corporation

FISCAL YEAR 2013

federal grant(s)/contracts	federal agency	dollar value	subject(s) of contract or grant
	CIVIL/Other US Government/Intelligence	$ 97,715,851.80	Information Technology Services
	Department of Defense	$ 11,938,062.87	Information Technology Services
	Department of Homeland Security	$ 1,091,747.66	Information Technology Services
	NASA	$ 455,861.47	Information Technology Services

FISCAL YEAR 2012

federal grant(s)/contracts	federal agency	dollar value	subject(s) of contract or grant
	CIVIL/Other US Government/Intelligence	$ 426,721,131.84	Information Technology Services
	Department of Defense	$ 51,686,883.38	Information Technology Services
	Department of Homeland Security	$ 501,061,811.62	Information Technology Services
	NASA	$ 1,858,850.31	Information Technology Services

FISCAL YEAR 2011

federal grant(s)/contracts	federal agency	dollar value	subject(s) of contract or grant
	CIVIL/Other US Government/Intelligence	$ 226,691,740.37	Information Technology Services
	Department of Defense	$ 47,916,332.50	Information Technology Services
	Department of Homeland Security	$ 118,090,215.57	Information Technology Services
	NASA	$ 49,924,335.63	Information Technology Services

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government: (Note: Unisys response is Awards received in the FISCAL YEAR)

Current fiscal year (2013):	96
Fiscal Year 2012:	281
Fiscal Year 2011:	256

Federal Agencies with which federal contracts are held: (Note Unisys response is the Agencies for Awards received in the subject FISCAL Year)

Current fiscal year (2013):	See above chart
Fiscal Year 2012:	See above chart
Fiscal Year 2011:	See above chart

List of subjects of federal contracts(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2013):	IT Services
Fiscal Year 2012:	IT Services
Fiscal Year 2011:	IT Services

Aggregate Dollars value of federal contracts held: (Note: Unisys response is Aggregate Dollars for Total Contract Value for the Fiscal Year Awarded.)

Current fiscal year (2013):	$	111,201,523.80
Fiscal year 2012:	$	981,328,677.15
Fiscal year 2011:	$	442,622,624.07

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subcontracts) with the federal government:

Current fiscal year (2013):	0
Fiscal Year 2012:	0
Fiscal Year 2011:	0

Federal Agencies with which grants are held:

Current fiscal year (2013):	N/A
Fiscal Year 2012:	N/A
Fiscal Year 2011:	N/A

List of subjects of federal grants(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2013):	N/A
Fiscal Year 2012:	N/A
Fiscal Year 2011:	N/A

Aggregate Dollars value of federal grants held:

Current fiscal year (2013):	N/A
Fiscal year 2012:	N/A
Fiscal year 2011:	N/A

House Armed Services Committee
Subcommittee on Intelligence, Emerging Threats and Capabilities
June 28, 2013

Past, Present, and Future Irregular Warfare Challenges: Private Sector Perspectives

Barry Costa
Director, Office of Technology Transfer
The MITRE Corporation

Chairman and members of the subcommittee, thank you for inviting me to speak today about irregular warfare challenges, specifically the value of sociocultural situational awareness and the technologies and data that enable this awareness and support rapid and effective decision making.

What I will describe is 21st century "radar" . . . i.e., technology that can provide us with rapid and effective insight into the changing scenarios for irregular warfare, as well as other missions. Just as airborne cameras give us a view of the physical terrain, there are now technologies that give us a view of the human terrain, including populations, networks, groups, and behaviors.

The ability to rapidly understand the human environment around the world is becoming increasingly important, as we have all seen in the past few years. It is critical to the security of the United States to understand the sentiments and actions of people throughout the world, and to be able to appropriately engage with words and deeds to positively shape the environment.

While technology can't replace deep human insight, MITRE firmly believes that understanding this human domain is possible and is best supported by technologies that are both empirically derived and scientifically grounded. What we have discovered, achieved, and transitioned in the past 10 years has shown great promise and applicability, despite just modest investments. There is a case to be made for continued, and perhaps larger, investments in this area so that additional progress can be made more quickly.

The not-for-profit MITRE Corporation operates a number of federal agencies' Federally Funded Research and Development Centers and manages an independent research and development program, which leads research in this area. In addition to conducting research, we help our government sponsors apply this new technology to their missions, including irregular warfare, counter-proliferation, counter-WMD, and even public interest healthcare issues. MITRE's "Social Radar" vision helped drive the Department of Defense's thoughts and investments in this area and, for that, we are proud.

To understand the global human environment, we need to look beyond the places in which the United States has forces, including Afghanistan, and consider all potential places for conflict, which could form very quickly. The technologies that MITRE and others have been developing and transitioning for the past several years are the principal tools of phase 0 military operations, when we must positively engage with allies and adversaries. The tools are also enablers for irregular warfare since they allow us to determine the networks, groups, key influencers, and audiences with whom we should engage.

We are also convinced that by working together with academia, industry, and government, we can more quickly bring the right combination of expertise together to solve these tough challenges and get capabilities into the hands of the warfighter. Collaborating

with this broad community also improves MITRE's ability to transition our intellectual property directly to sponsors and industry, when appropriate. By transferring our technology to customers, other U.S. government agencies, commercial entities, and academia, these tools can be of broad value to our sponsors and the U.S. government.

As we continue to research and transition social radar tools and technologies, we look to increase affordability and effectiveness by finding new ways to use these technologies to support multiple mission domains.

It was more than 10 years ago, when working on a U.S. Special Operations Command (USSOCOM) program, that we began to envision and build tools to provide insights into the human domain. Six years ago we helped the Department of Defense (DoD) begin and execute the Human Social Culture Behavior Modeling Program. This led to the creation of indications and warning capabilities that can alert us to significant changes in the human environment, such as long-term worldwide instability or the kind of changes we saw during the Arab Spring. Over these 10 years, the DoD has made great progress with a modest investment, but there is much more to be done.

The need for these capabilities was publicly recognized around 2006, after years of experience with non-conventional conflicts spanning multiple operational phases in culturally complex and unfamiliar terrain in Iraq and Afghanistan. These years gave the U.S. military a deep appreciation for the importance of sociocultural understanding. Success in these conflicts depended on close, effective interaction with an array of actors, including local populations, governments and military forces, allies, and non-governmental groups.

This experience led an increasing number of military leaders to

articulate the need for enhanced capabilities rooted in social and cultural factors to understand behaviors. For example, when Lieutenant General Benjamin Freakley was in Afghanistan as Commanding General Combined Joint Task Force-76, he said, "We must develop the ability to understand the complex human factors and must incorporate them into all facets of operations."

Overall in the last six years, the defense community has built a science and technology foundation for understanding this human domain and has improved capabilities for understanding behaviors driven by social and cultural variables. We are now better positioned to pursue effective courses of action in the full range of military operations. In fact, the research community has already delivered some of these tools to organizations including: USSOCOM, as well as the U.S. Southern, Strategic, and Pacific Commands, International Security Assistance Force, and U.S. Army Training & Doctrine Command Analysis Center. The adoption of these technologies is not limited to the Department of Defense; the Intelligence Community and Department of State are also adopting technologies in this domain.

Much remains to be done, however, to evolve and adapt sociocultural behavior sense-making capabilities to play a vital role in current and future missions. Recent, rapid, and profound shifts in the geo-political context have brought renewed attention to challenges such as hostile non-state actors who may be pursuing weapons of mass destruction, nation-state instability driven by drug economies and transnational criminals, humanitarian and disaster relief, and cyber threats. Continued sociocultural behavior research can make significant contributions to all of these missions.

The nation must adapt its methods and create new tools that reflect the realities of national security in the new age of real-time global information flow, and we must understand and engage in the public dialogue created by these new communication media.

While social media is only one of many different data sources necessary to achieve this human domain awareness, and is best used in conjunction with traditional data and methods, its importance is growing rapidly. It is a wired world in which 2 billion people have mobile broadband and 4.8 billion people have cellphones. We expect most of the world's population to be connected to the internet in some way within the decade. As this happens, more and more people will use social media and similar mechanisms to describe their locations, themselves, and their environments.

The challenge is to find the valuable signals amidst an enormous amount of data. Lieutenant General Michael Flynn, Director of the Defense Intelligence Agency, has argued that we "must develop a sensory capability to better detect the precursors to political change, a social radar that enables policy leaders to make informed decisions that maximize national influence left of bang."

There are many very difficult challenges in this area, some of which will take decades to solve, but there are things we can do now to detect meaningful signals amidst the data deluge, support more timely alerting of change, and better understand the effectiveness of our words and actions upon various audiences.

The Assistant Secretary of Defense Research & Engineering's Human Social Culture Behavior Modeling Program drove many of today's successes, including the Worldwide Integrated Crisis of Early Warning System (W-ICEWS), which forecasts long-range nation state instability, and the Identifying and Countering Terrorist Narratives project, which allows us to go beyond what is explicitly stated and understand the deeper underlying narrative. In addition, the program developed network-based metrics for discovering change in dynamic networks and identification of emergent leaders, issues, and trends; and it developed a simulation-based workbench combining computational models that allows

users to experiment with the effectiveness of alternative actions to influence audiences.

In addition, MITRE has developed proof-of-concept Social Radar tools that support understanding of rapidly changing sentiment and emotion across the globe.

Innovative ideas for research, science, and technology are essential to long-term success in building DoD sociocultural behavior capabilities. Experience to date suggests an exciting future in which global information, applied research, and analytics are fully and dynamically integrated. However, DoD and the nation are not at that desired end-state. To get closer, DoD should maintain the momentum created over the past several years by supporting promising research thrusts that will result in the capabilities most relevant to future national security demands.

The recommendations that follow reflect the experience of the last six years in the Human Social Culture Behavior Modeling project, including our understanding of current commercial technology and research efforts under way in this domain.

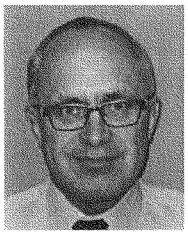
1. DoD needs a robustly funded research and engineering program to address the range of capabilities users need. The area of applied sociocultural behavior research and engineering is still relatively young. Specified requirements remain relatively limited, despite widespread acknowledgment of needs. While the Services are conducting research in this domain, funding cuts have blunted the creation of the scale of programs needed.
2. The Services should prioritize Science & Technology for the development of sociocultural behavior capabilities, building on some of the innovative work already under way. This needs to be supported by specification of current

sociocultural behavior-related capabilities and the requirements of Service communities. To maximize the success of the first two recommended actions, DoD needs to intensify coordination across the sociocultural behavior research space. Using mechanisms such as the Office of the Secretary of Defense Human Systems Social, Cultural and Behavioral Understanding sub-area group, DoD should increase coordination both horizontally (across the Services and at any given level of research) and vertically (from Basic through Applied research and on to Advanced Technology Development and Prototyping programs).

3. DoD should identify a center of excellence for sociocultural modeling, integration and analysis, focused on application of technology to user needs, rapid transition to users and Programs of Record, metrics, data interoperability, model validation, and model reuse and generalizability. This center should emphasize moving sociocultural behavior tools into operations as quickly as possible.

Let me leave you with this thought: If the DoD had ended its research investment in pulsed radar technologies after just five years, the program would have ended in 1939, at the start of World War II, leaving us with a rudimentary capability for long-range sensing, as well as a glimmer of its tantalizing potential.

The research in human domain situational awareness may prove just as important. We must continue to support this research, as well as the quick transition of capabilities to the organizations that need them.



Barry Costa
Director, Technology Transfer Office

Barry Costa leads MITRE's program to transfer MITRE-developed technology directly to the government or to industry, which then makes these technologies available to the government and the public as affordable products. The Technology Transfer Office works closely with MITRE's engineers and scientists to guide them through the transfer process, as well as with organizations who are interested in licensing our technology or in collaborating on its development for the government's benefit.

Mr. Costa also serves as the director of MITRE's Corporate Initiative on Smart Power and as the systems engineer for the Assistant Secretary of Defense Research & Engineering's Human Social Culture Behavior modeling program. In addition, he leads a MITRE research portfolio of projects in the Human Geography and Smart Power domains. His current technical focus is on the research and transition of natural language processing and sociocultural understanding and modeling capabilities, with an emphasis on the development and transition of such systems for operational support.

Since joining MITRE in 1984, Mr. Costa has led critical, fast-paced projects for the Air Force, Joint Staff, U.S. Central, Atlantic, and Special Operations Commands, as well as other organizations. He has had a broadly diverse career in pioneering technologies for: digital imaging and immersive visualization systems, human social culture behavior analysis and modeling, operationally focused technical analyses, and radar modeling.

Mr. Costa has worked in a wide range of technologies over his career at MITRE, continually looking for ways to combine his experiences to find innovative solutions for our sponsors. His projects have included doing systems engineering for programs such as the Aegis Combat System and Joint Surveillance Target Attack Radar System; designing computer networks and communications architectures; helping U.S. Central Command prepare communications systems for Desert Storm; integrating and managing multimedia data collections; designing tactical video systems and imaging systems; and developing software prototypes for data extraction and analysis.

Before joining MITRE, Mr. Costa served on active duty with the U.S. Navy. He is a graduate of the University of Massachusetts at Amherst.

DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 113th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee.

Witness name: Barry A. Costa
Capacity in which appearing: (check one)

___Individual

_X_Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: The MITRE Corporation

FISCAL YEAR 2012

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
2	DOD	941,174,299	R&D
1	DHS	78,202,089	R&D
1	FAA	149,396,674	R&D
1	Department of Treasury	155,132,098	R&D
3	VA	71,237,801	R&D
2	Department of State	1,192,121	R&D
1	NOAA	1,087,254	R&D
1	NASA	192,518	R&D
1	NSF	16,986	R&D
1	Department of Agriculture	2,964	R&D
1	Department of Energy	95,810	R&D
1	Administrative Office of the United States Courts	5,308,534	R&D
1	Undersecretary of Defense - JASONS	5,801,646	R&D

FISCAL YEAR 2011

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
2	DOD	934,335,591	R&D
1	DHS	86,330,219	R&D
1	FAA	154,642,179	R&D
1	Department of Treasury	126,639,144	R&D
3	VA	60,571,158	R&D
2	Department of State	2,189,406	R&D
1	NOAA	1,432,558	R&D
1	NASA	136,543	R&D
1	NSF	14,481	R&D
1	Department of Agriculture	1,945	R&D
1	Administrative Office of the United States Courts	4,650,480	R&D
1	Undersecretary of Defense - JASONS	4,940,629	R&D

FISCAL YEAR 2010

Federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
2	DOD	916,969,182	R&D
1	DHS	59,803,132	R&D
1	FAA	141,978,500	R&D
1	Department of Treasury	142,905,285	R&D
2	VA	27,036,785	R&D
2	Department of State	1,942,284	R&D
1	NOAA	2,350,237	R&D
1	NASA	383,748	R&D
1	NSF	119,143	R&D
1	Department of Agriculture	1,328	R&D
1	Undersecretary of Defense - JASONS	5,698,003	R&D

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2012): 17
Fiscal year 2011: 16
Fiscal year 2010: 14

Federal agencies with which federal contracts are held:

Current fiscal year (2012): See above
Fiscal year 2011: See above
Fiscal year 2010: See above

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2012): R&D
Fiscal year 2011: R&D
Fiscal year 2010: R&D

Aggregate dollar value of federal contracts held:

Current fiscal year (2012): $1,408,840,794
Fiscal year 2011: $1,375,884,333
Fiscal year 2010: $1,299,187,735

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2012): 1
Fiscal year 2011: 1
Fiscal year 2010: 1

Federal agencies with which federal grants are held:

Current fiscal year (2012): NSF
Fiscal year 2011: NSF
Fiscal year 2010: NSF

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2012): Collaborative R&D
Fiscal year 2011: Collaborative R&D
Fiscal year 2010: Collaborative R&D

Aggregate dollar value of federal grants held:

Current fiscal year (2012): $16,986
Fiscal year 2011: $14,481
Fiscal year 2010: $119,143

STATEMENT BY

SCOTT E. JACOBS PRESIDENT, NEW CENTURY US

BUILDING INTELLIGENT CAPACITY

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES
COMMITTEE ON ARMED SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

112TH CONGRESS

ON

PAST, PRESENT, AND FUTURE IRREGULAR WARFARE CHALLENGES: PRIVATE SECTOR PERSPECTIVES

JUNE 28, 2013

NOT FOR PUBLICATION

UNTIL RELEASED BY THE

COMMITTEE ON ARMED SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

Mr. Chairman, Ranking Member Langevin, members of the subcommittee, I thank you for the opportunity to appear before this panel today. As a retired Federal special agent and as a graduate of the congressional fellowship program, I am acutely familiar with the leadership provided by this committee. As the current President of New Century US (NCUS), I would like to personally thank each and every one of you for your steadfast dedication to public service.

Introduction

New Century US is a privately-held firm currently on contract with the U.S. government to provide, among other things, training and education support to the Afghan National Army(ANA). NCUS is the American subsidiary of the London-based New Century International and has been founded in a manner consistent with all laws, regulations, and protocols established by the U.S. government. The firm is proud of the variety of services it provides in support of the U.S. government and its allies. In support of the NATO mission in Afghanistan, New Century International currently provides training and mentoring support to the Afghan National Police (ANP). NCUS has also provided a similar service to authorities in a vis-à-vis a "train-the-trainer" program, an initiative authorized and funded through the DoD Counter Terrorism Technical Support Office for the U.S. military. Furthermore, NCUS continues to provide high-quality operations' analysis and intelligence-related support to a variety of other federally-funded initiatives. In sum, the firm's programs and the nature of the collective experience of New Century personnel, positions the firm as both an observer of irregular challenges worldwide and as a knowledgeable proponent of irregular solutions.

Current Activities

The flagship program of our firm is called "Legacy," a program first implemented in the western Iraq province of al Anbar and currently in place in Afghanistan. Aimed at improving both the capability and capacity of the ANP and ANA forces, the current iteration of Legacy employs a specific doctrine and

teaching methodology, one based on the experience of the British constabulary force – or Special Branch – in Northern Ireland during the conflict of the late 1970s and '80s.

The value-added of the New Century approach lies not only in its well-developed Legacy methodology but also – and most importantly – depends on its deep well of experience found within the ranks of qualified personnel. As I previously mentioned, the success of the firm rests with "doers" – several veterans of Special Branch and the Northern Ireland conflict, as well as others more recently seasoned after years of serving in Iraq and Afghanistan. Indeed, the doctrine and methodology of the Legacy program is designed to leverage and reflect the richness of this experience. The curricula of the respective programs thus includes both in-class discussion and the all-important, in-the-field "hands on" training.

New Century provided training has produced a number of quantifiable results in support of the NATO mission in Afghanistan. By adapting traditional Special Branch tactics, techniques, and procedures (TTPs) to accommodate and befit the unique circumstances of the local culture, the Legacy methodology has developed and nurtured an ever-diligent, wiser, and more coordinated Afghan police force. Since inception, the Afghan Legacy program has directly facilitated the capture of numerous improvised explosive devices, detonators, suicide vests, munitions, and other weapons. Furthermore, the resulting police force developed and tutored by our small, hybrid teams of cultural advisers and former special police personnel has been responsible for the arrest, capture, or death of more than six hundred insurgents. We remain honored and humbled by the following praise offered by a former 3-star American General at the beginning of the effort: "New Century's program is immediately effective."

But the greatest achievement of Legacy, we believe, lies in the much-improved reporting and increased coordination apparent throughout the larger ANP community, *and* in the effective fusion of military, intelligence, and law enforcement TTPs in support of a larger counter-insurgency (COIN) and

counter-terrorism mission. We believe our hybrid approach is notably consistent with David Kilcullen's views about the prerequisites of an effective COIN strategy when he writes in his book, *Accidental Guerilla*:

> "[P]olice intelligence analysts are a good first step, and the police intelligence capability should grow naturally to include informant networks, undercover police officers, and *joint police-military intelligence centers.*"[1]

We also agree with the counsel of National Defense University professor Bard E. O'Neill when he argues in favor of creating such a force before the onset of an insurgency:

> "[W]ise governments turn to specially trained police and intelligence agencies for a solution...Keeping the military out of the day-to-day business of countering terrorists in favor of special police forces can be done even when the latter are part of the military establishment."[2]

And so, at New Century we believe a focus on improving the capacity of the Afghan – and other host-nation – security forces is a wise and an intelligent investment for supporting American foreign policy objectives, as it also offers the potential to build an effective residual or "leave-behind" security force when a U.S. military presence is reduced or simply unavailable. As U.S. taxpayers, we also view this approach as a wise and cost-effective investment strategy for leveraging limited public resources.

The Strategic Landscape

The firm believes in, embraces, and supports the all-important "by, with, and through" creed of the Special Operations Forces community as it applies to meeting U.S. foreign policy objectives. We view this indirect approach as practical and essential for working with foreign allies, as well as for identifying and confronting irregular challenges around the globe – especially in environments requiring a limited

[1] David Kilcullen, *The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One*, New York: Oxford University Press, 2009, p. 61.
[2] Bard E. O'Neill, *Insurgency and Terrorism: Inside Modern Revolutionary Warfare*, Dulles, Va.: Brassey's, 1990, p. 129.

counter-insurgency response. And because both irregular threats abroad and federal budget pressures at home are almost certain to continue, we believe the indirect and *irregular* approach will become even more important in the days ahead.

Terrorism, insurgency, crime, and the illicit trafficking of drugs and humans – these are the activities that promise to litter the global strategic landscape in the years ahead. They already exist today in too many regions of the world – in Africa, South America, and across Asia – where weak nation-states are incapable of mounting an effective response. If ignored or unassisted, some of these states may falter and fail and follow the path of Afghanistan in the 1990s or of Somalia today – enlarging evermore that part of the world in which American ideals and interests are threatened or under siege. A carefully-targeted assistance program, therefore, would be wise, one designed to develop and empower the local authorities of American allies. Just imagine the strength of America's strategic position if the local authorities in the following nations simultaneously mounted with U.S. assistance a more effective and sustainable counter-terrorism and COIN program: Uganda, Tanzania, Mali, the Central African Republic, Chad, Peru, Thailand, and the Philippines. Imagine, too, the improved security posture and greater moral authority of America if both the U.S. State Department and the Department of Defense (DoD) combined efforts and jointly offered security reform assessments to potential partners and allies around the globe.

Lessons Learned and Recommendations for the Future

The Afghan Legacy program adopted the same goals as those of the original program in Iraq: first, develop a locally-based human collection and analysis capability; and second, establish an information-gathering and investigative infrastructure within the police to support COIN strategic objectives. We believe we achieved both of these objectives and have learned a number of important lessons about COIN and Irregular Warfare (IW) along the way.

First, a thorough understanding of both the local- and national-level strategic environments is essential and enhances the performance of the small, hybrid teams of mentors and advisers. This requires keeping an eye on both the larger picture and strategic aim while examining and researching the local networks and possible biases of families, tribes, and local leaders. A thorough understanding of the environment also allows a training team to keep a focus on the proper objectives throughout the full spectrum of the program's performance, or from the early stages of planning through actual training, implementation, and review. This level of understanding can be produced by an initial assessment conducted by a small advance team of researchers.

Second, designing and tailoring a flexible doctrine and training regime increases local acceptance of the program. In Iraq, we noticed that trainees were *experiential* learners and responded best to role-playing scenarios and also responded well to stories about veteran experiences in the Northern Ireland campaign. In Afghanistan, we discovered and thus designed and implemented a simpler and streamlined reporting methodology, one more suitable to a culture with such a low literacy rate.

Third, in COIN campaigns the timely reporting of information is necessary for it to be useful or actionable, placing a premium on adequate communication habits and requiring a close relationship between the trainers and the trainees.

Fourth, future field surveys and training efforts should also assess the natural respect for the rule of law in a specific country and lend attention to the workings and integrity of the judicial branch of government.

Fifth – and this is important – for a Special Branch-like activity to ultimately succeed the U.S. military must embrace it as part of an overall COIN doctrine and strategy, budget and train for it, and

provide daily support for it in the field. Failure to provide adequate transportation and security support, for instance, might derail the entire effort.

Sixth, effective COIN efforts may take time and require patience. The British success in Northern Ireland, for example, took over two decades to secure. Therefore, U.S. policymakers should also consider preventive programs along the lines of Professor's O'Neill's counsel and remain mindful of the following phrase: "an ounce of prevention is worth a pound of cure."

A final observation is actually a concern and pertains to the point just made about doctrine, training, and budgeting for such a capability. Despite significant gains in the field and notwithstanding the 2008 issuance of a DoD Directive on IW (i.e., 3000.07), the department and each of the military services have remained somewhat listless with respect to this important subject. The 2008 Directive assigned additional duties to both Special Operations Command and the Office of the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict, granting these organizations lead roles for defining, guiding, and coordinating IW-related activities across DoD. And yet five years later, we still do not see any tangible leadership on these issues anywhere in the department. The 2010 Quadrennial Defense Review and the 2012 Defense Strategic Guidance only lightly referenced the concept, and no true champion has emerged for institutionalizing such lessons or for providing a sustainable budget.

Final Thoughts

The complex nature of the world requires innovative solutions. At New Century we strongly believe a large part of the solution lies in the fusion of the conventional and the unconventional, in both the regular and the irregular, and in a greater collaboration between the communities of law enforcement, intelligence, and military professionals. We also believe in the use of small, highly-

experienced training teams for building the capacity of our allies, and for constructing a defensive network of collaborators in various hotspots – or potential hotspots – around the world.

In a recent on-line article retired General Stan McChrystal noted that it takes a network to defeat a network, and this is precisely the situation we find ourselves in today.[3] Ironically, his comment echoes language authored by this subcommittee and included in the House reports accompanying passage of both the 2011 and the 2012 National Defense Authorization Acts:

> "The committee remains concerned that the Secretary of Defense has not taken full advantage of a novel approach that takes into account an understanding of the tribal landscape and invests in developing host nation security forces, particularly local police organizations that maintain close ties with and function to protect the local population. The committee praised this approach, the Legacy program, in the committee report (H.Rept. 111-491) accompanying the National Defense Authorization Act for Fiscal Year 2011. In the report, the committee noted special interest in the "Attack of the Network" approach used in the Republic of Iraq and Afghanistan under the Legacy program. Accordingly, the committee directs the Secretary of Defense to conduct an assessment of the following:
>
> 1) The applicability of the Legacy program in other operations and regions where networked based threats are present or where conditions are conducive to supporting these threats; and
> 2) Options for an appropriate management structure within the Department to institutionalize and sustain the capabilities that Legacy and similar programs provide."[4]

At New Century we agree with both this assessment and General McChrystal's assertion and have come to this conclusion after years spent toiling in the field. We feel that the combination of our unique methodology and depth of experience offers the perfect recipe for disrupting the forces of terrorism, crime, and subversion. But more visionary and effective leadership is needed in the U.S. government, just as more international partners and allies are required. Our nation cannot do it alone.

---

[3] Stanley McChrystal, *Lesson from Iraq: It Takes a Network to Defeat a Network*, http://www.linkedin.com/today/post/article/20130621110027-86145090-lesson-from-iraq-it-takes-a-network-to-defeat-a-network?trk=eml-mktg-celeb-sc-prehed (June 2013).

[4] *The National Defense Authorization Act for Fiscal Year 2011*, http://www.gpo.gov/fdsys/pkg/CRPT-111hrpt491/pdf/CRPT-111hrpt491.pdf; *The National Defense Authorization Act for Fiscal Year 2012*, http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt78/pdf/CRPT-112hrpt78.pdf.

"By, with, and through," is an effective guiding principle for the United States in the years ahead. We recommend that we follow it.

Scott E. Jacobs

Professional Profile

Results driven executive with a history of achievement in driving innovation and partnerships. Proven capacity to envision and direct national security projects and first of their kind business development initiatives. Experienced leader managing operations for small businesses to include launching new products and successfully managing client relationships. Core competencies include:

•Strategic planning and execution • Influential change leader • Decisive business leadership

Experience and Achievements

NEW CENTURY US, Arlington, VA **2011 – current**
A company focused on security sector reform initiatives that trains and mentors law enforcement personnel in third world countries to build rule of law processes and improved law enforcement capacities. ($7M)
President
Report to Board of Directors with responsibility of expanding business, reducing costs, building a corporate team and execution on contracts while maintaining quality and customer satisfaction.

- Increased net profits by 18 percent.
- Maintained safety and security of personnel in semi permissive environments.
- Exceeded performance metrics in developing law enforcement capacity with host nation authorities.

INTELLICHECK MOBILISA, Alexandria, VA **2010 – 2011**
An identity management and access control software company providing access control solutions to the Department of Defense and commercial enterprises.($20M/software manufacturer/reseller/200+ customers)
Senior Vice President, Defense ID Group
Recruited by CEO to orchestrate a complete turnaround and revitalization of the Defense ID Group as part of company's plan to increase revenues in the government market. Realigned positions, staffed key business development positions, redefined performance goals and instilled a culture of customer-centric performance excellence. Led a team of software developers/engineers, sales professionals, marketing and technical support staff in the sales and installation of products throughout the DoD and the development of new products based upon changing customer requirements.

- Achieved 1st year revenue growth of 5 percent within 8 months, exceeding corporate expectations.
- Launched Fugitive Finder a new Defense ID product successfully.
- Partnered with key prime contractors on government contract proposals valued at $32 million dollars.

21ST CENTURY SYSTEMS INCORPORATED (21CSI), Arlington, VA **2009 – 2010**
A decision support software product and geospatial services company managing $20 million in revenue having 9 offices and 150 employees delivering products to the U.S. military.
Senior Vice President, Federal Systems Group (FSG)
Reported directly to CEO acting in the capacity of a Chief Operations Officer directing a staff of 4 Vice Presidents with responsibility for 24 software and geospatial development projects and day to day company operations.

- Led the FSG by increasing productivity by 7 percent, delivering quality products on time and on budget.

- Drove initiatives that reinvested $3 million in internal research and development funds to maintain competitive edge on product line.
- Collaborative business partner with track record for fostering relationships with prime contractors, vendors and employees to deliver sustainable ROI and gain new market share.

NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS) **1981 -2008**
NCIS is a worldwide law enforcement, counterterrorism and counterintelligence organization with a presence in 41 countries and 160 locations.

Director, (Acting), DoD Counterintelligence Field Activity (CIFA), Arlington, VA **2008**
Director, CIFA reports directly to the Undersecretary of Defense for Intelligence and is the program manager for the DoD counterintelligence (CI) enterprise, leading approximately 900 CI specialists in the management and execution of the national CI strategy.

- Served as principle advisor to the Undersecretary of Defense on all CI matters.
- Responsible for the integration of CI activities, execution of CI priorities, management and advocacy of CI funding programs and resources.
- Directed the day to day operations of all CIFA personnel, resources, programs and activities.

Executive Assistant Director, Senior Executive Service, Combating Terrorism Directorate 2005-2008
Led the agency's Combating Terrorism Directorate consisting of 450 government and contractor personnel in the investigation of all terrorism incidents and operations impacting the Navy/Marine Corps personnel.

- Directed all high level investigations/operations and communicate findings to senior government leaders.
- Responsible for DON policy on critical infrastructure protection, force protection, protective service, biometric, identity management and vulnerability assessment programs.
- Launched an innovative enterprise solution for DoD suspicious incident reporting with the FBI.

Special Agent in Charge, Northwest Field Office, Silverdale, WA **2001-2005**
Leader of an office consisting of 100 criminal investigators, counterintelligence, counterterrorism and force protection professionals that serviced 75 Navy commands in a five state region.

- Formed the first law enforcement information sharing consortium in the country—Northwest Law Enforcement Information Exchange (LInX)—consisting of approximately 150 federal, state and local law enforcement agencies. Currently deployed to 9 regions throughout the United States.
- Identified and launched a $5 million effort to develop access control technologies to protect Navy bases.

Deputy Assistant Director, Economic Crimes Department, Washington, D.C. **1996-2000**
Legis Fellow, Brookings Institution, Washington, D.C. **1995-1996**

Education and Affiliations

MA, Washington State University, School of Criminal Justice, 1980
BA, Criminal Justice with honors, Phi Beta Kappa, Washington State University, 1978
Certificate, DoD National Security Management Course, Maxwell School, Syracuse University, 1995
Certificate, DoN Flag Officer Training Course, Shepardstown, WV, 2004
Certificate, DoN Executive Business Course, University of North Carolina, Chapel Hill, 2007
Member, International Association of Chiefs of Police

DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 113th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee.

Witness name: Scott E. Jacobs

Capacity in which appearing: (check one)

___Individual

_X_Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: New Century U.S.

FISCAL YEAR 2013

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Combined Security Transition Command-Afghanistan (CSTC- A)	U.S. Army	$6.5 million	Mentoring and advising the Afghanistan National Army
Advanced Security Force Assistance Capability Development (ASFACD)	Department of Defense Special Operations and Low-Intensity Conflict , Combating Terrorism Technical Support Office	$139,334	Training and mentoring framework for U.S. Forces while working in conjunction with host nation security forces.

FISCAL YEAR 2012

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Combined Security Transition	U.S. Army	$6,086,589	Mentoring and advising the Afghanistan National Army

Command-Afghanistan (CSTC- A)			
Advanced Security Force Assistance Capability Development (ASFACD)	Department of Defense Special Operations and Low-Intensity Conflict , Combating Terrorism Technical Support Office	$300,666	Training and mentoring framework for U.S. Forces while working in conjunction with host nation security forces.

FISCAL YEAR 2011

Federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Combined Security Transition Command-Afghanistan (CSTC- A)	U.S. Army	$5,913,544	Mentoring and advising the Afghanistan National Army

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2013): 2 ;
Fiscal year 2012: 2 ;
Fiscal year 2011: 1 .

Federal agencies with which federal contracts are held:

Current fiscal year (2013): U.S. Army; Department of Defense Special Operations and Low-Intensity Conflict Combating Terrorism Technical Support Office ;
Fiscal year 2012: U.S. Army; Department of Defense Special Operations and Low-Intensity Conflict Combating Terrorism Technical Support Office ;
Fiscal year 2011: U.S. Army.

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2013): training and mentoring;
Fiscal year 2012: training and mentoring;
Fiscal year 2011: training and mentoring.

Aggregate dollar value of federal contracts held:

Current fiscal year (2013): $6,639,334 ;
Fiscal year 2012: $6,387,255 ;
Fiscal year 2011: $5,913,544 .

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

Federal agencies with which federal grants are held:

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

Aggregate dollar value of federal grants held:

Current fiscal year (2013):_____;
Fiscal year 2012:_____;
Fiscal year 2011:_____.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

JUNE 28, 2013

RESPONSE TO QUESTION SUBMITTED BY MR. FRANKS

Mr. JACOBS. See attached. [See page 22.]

New Century
BUILDING INTELLIGENT CAPACITY

The Legacy Program in Afghanistan: Selected Statistics and Successes

Prepared for Members of the House Armed Services' Intelligence, Emerging Threats & Capabilities Subcommittee

For Official Use Only www.newcentcorp.com July 2013

New Century
BUILDING INTELLIGENT CAPACITY

INTRODUCTION

At the June 28, 2013 hearing on *Past, Present, and Future Irregular Warfare Challenges: Private Sector Perspectives,* Congressman Trent Franks requested New Century's representative, Mr Scott Jacobs, to provide statistical information evidencing the claimed successes of the Legacy program in Afghanistan.

In this document we provide a selection of such statistics and related narrative reporting on intelligence-led operations mounted by the Afghan National Security Forces (ANSF) stemming from the mentoring and training delivered by the Legacy program. New Century is not privy to ISAF's tracking and analysis of the program's performance, therefore, what is presented here is only a partial picture of the operational activities, being one assembled from our own internal reporting.

STATISTICS

In accordance with our program performance obligations, each mentor routinely submits highlights report. The following three tables set out a selection of performance achievements gleaned from these reports, covering a three year period to June 2013. The actual numbers will be higher but the information provided is the cumulative values of what we are able to track from the content of the mentor reports.

We do not have access to data on the number of sources recruited or the number of intelligence reports filed (albeit the latter is understood to be significant).

Recoveries – IED-related	Cumulative
IEDs (complete)	1,083
Suicide vests (complete)	29
Explosives (kg)	13,850
Mines (various)	158
Warheads (various)	1,159
Mortar rounds	537
Detonators	479
Ammonium Nitrate (kg)	50,600

Recoveries – Other	Cumulative
RPG Launchers	34
Weapons (light up to AA guns)	574
Ammunition rounds (various)	32,270
Grenades	179
Radio units	84
Vehicles	51

New Century
BUILDING INTELLIGENT CAPACITY

Recoveries – Other	Cumulative
Drugs (various) (kg)	1,908
Stolen goods (USD value)	8,000,000

Other Factors	Cumulative
Insurgents arrested	483
Insurgents KIA	159
IED factories identified	4
Drug processing labs shut	2
Kidnap victims recovered	5

The above recoveries and removal of Taliban operatives has undoubtedly led to the protection of numerous lives, both those of Coalition / Afghan Forces and civilians alike. Taking just the IED statistic in isolation and applying a subjective factor of one death avoided for each IED recovered would suggest that at least 1,000 lives have been saved from this factor alone.

The Legacy program comprises the two principal components of: (1) mentoring in the field (with a 24/7 availability); with (2) classroom training in the designated schoolhouses. Below is a table of the courses run between April 2010 and June 2013 under the classroom component. Key statistics to note are that 323 courses were delivered, spanning 25 course titles, provided to more than 3,000 students, and in excess of 61,000 student training days completed.

Course Title	Average Days Duration	Students per Course	Number Courses Run	Training Total Days	Number Students Trained	Student Total Days
Basic Source Management	19.9	9.6	119	2,373	1,145	22,415
Intermediate Source Management	20.2	6.7	35	708	233	4,748
Introduction to Intelligence	7.0	6.0	1	7	6	42
Combat Intelligence	13.0	26.0	1	13	26	338
HUMINT Collector	37.1	14.0	10	371	140	5,222
HUMINT Collector (MICO)	29.2	18.5	22	643	407	11,812
Advanced HUMINT Collector	28.2	9.6	5	141	48	1,347
Source Debriefing	14.0	19.0	1	14	19	266
Surveillance Intel Officer	13.0	6.0	1	13	6	78
Basic Foot Surveillance	22.7	8.0	3	68	24	544
Basic Mobile Surveillance	36.4	7.8	5	182	39	1,429
Intermediate Surveillance	62.0	9.0	2	124	18	1,116
Map Reading and GPS	6.3	8.8	11	69	97	654

New Century
BUILDING INTELLIGENT CAPACITY

Course Title	Average Days Duration	Students per Course	Number Courses Run	Training Total Days	Number Students Trained	Student Total Days
Photography Familiarization	1.0	7.7	3	3	23	23
Surveillance Support	15.4	14.6	10	154	146	2,534
Collator	15.5	7.0	27	418	189	3,345
Analyst	17.4	7.7	13	226	100	1,732
Zone Desk Officer	14.2	12.3	6	85	74	1,006
Authorizing Officer	6.0	5.0	2	12	10	60
Report Writing	4.2	5.9	28	118	164	691
Management Induction	4.8	9.6	5	24	48	229
Manager's Awareness	5.4	8.6	7	38	60	305
SOF Capability Brief	53.0	11.5	2	106	23	967
Train-the-Trainer	20.7	5.7	3	62	17	351
Management Train-the-Trainer	9.0	6.0	1	9	6	54
		Totals	**323**	**5,981**	**3,068**	**61,308**

The Legacy program presently (July 2013) deploys 125 Subject Matter Experts (SMEs) in Afghanistan, of which a little over one-quarter are trainers delivering the above courses, with the vast majority of the remainder being mentors who work in the field alongside their ANSF counterparts, applying the Tactics, Techniques and Procedures enshrined in the written doctrine and supplemented by the provision of a catalog of hip-pocket lessons. The number of SMEs is expected to reduce in the coming months as the availability of force protection and life support diminishes as a consequence of the drawdown of Coalition Forces.

NATIONAL TARGETING AND EXPLOITATION CENTER (NTEC)

A central component of the transition of the Legacy program's intelligence capability to the ANP Directorate of Police Intelligence (DPI) has been the development of the Network Targeting Exploitation Center (NTEC) in Kabul. New Century has contributed to the technical expertise underpinning the establishment of this intelligence fusion and operations center through the mentoring of operational commanders and personnel, supported by guidance on the drafting of protocols for the management of the internal operational and administrative processes.

The New Century mentors working in the NTEC have capitalized upon the experience gained from operating within an equivalent, highly successful framework in the UK, particularly in Northern Ireland, to provide the ANSF with the capability to receive, analyze, plan and execute intelligence-led operations, each underpinned by legal warrants, and to do so in a coordinated and controlled manner, with the proper oversights mechanisms in place.

The process is based upon the original UK-based Tasking and Coordination Group (TCG) model to harmonize intelligence received within NTEC from a range of organizations / sources and enable the conduct of de-conflicted covert and overt policing operations. The Legacy program has assisted the DPI develop effective internal mechanisms for the flow of intelligence from ANSF source handlers, through intelligence analysts within the NTEC, to operational decision-makers. These processes have enabled decisions to be taken by ANSF commanders to risk assess, plan missions and then deploy specialist personnel, including surveillance teams, to proactively exploit intelligence opportunities.

Amongst the impressive statistics for the NTEC since it became operational two years ago is that, as of late June 2013 a total of 175 operations have been planned or are in plan, of which 107 have so far been completed. All operations are warrant-based, so have full legal standing. They have led to the arrest of 88 insurgents, with 21 more KIA. At least 35 IEDs have been recovered, along with suicide vests and numerous weapons, ammunition of various types, grenades, mines and warheads, plus 3,000kg of drugs and chemicals. Of course, these statistics present only part of the story as the effective disruption of terrorist acts will be causing disorientation and a number of such intended acts will simply not be undertaken for fear of interdiction or arrest.

Successes

The internal highlights reports filed by mentors includes narrative information on selected operations arising from intelligence collected by their mentees. These reports are assimilated by the program's technical support team and in the text below we have provided examples from two recent months (chosen at random) of these typically 10 page long documents.

December 2012 Examples

December 1: A HUMINT platoon member of forward deployed 207th Corps, MICO 1, Multi-Function Team (MFT) received intelligence from a source that Taliban had emplaced an IED next to the home of a well-known and wealthy individual in XXX in order to target ANSF/ANP personnel. This information was immediately passed to local ANA Operations center and to the ANP. The IED was discovered by local ANP and subsequently destroyed in situ.

December 6: Source intelligence was received that Taliban had emplaced 4x PPIEDs on a 50 meter stretch of road in XXX village, XXX district, XXX province. As a result of this intelligence a search was commenced. The search team located all four of the PPIEDs with pressure plates attached. All four IEDs were destroyed in situ.

December 6: XXX DPI received source intelligence that Taliban had emplaced 3x RCIEDs at XXX bridge, XXX village, XXX district. As a result of this intelligence a search was commenced. The search team located all three devices, consisting of 2x 10ltr and 1x 20ltr jugs. All three IEDs were destroyed in situ.
December 6: Source information indicated that Taliban were fabricating PPIEDs in a deserted compound in a named location in XXX district, XXX province. The compound belonged to XXX ALP Commander XXX, an ex-Taliban Commander who joined the reintegration process last year. As a direct result of this intelligence, AUP supported by ANA, ALP and NDS commenced a search of the grid location. The search team located 12x complete PPIEDs and 2x RPG rounds. The RPG rounds were detonated in situ and the 12x PPIEDs were transported to XXX AUP DHQ for disposal by US Military EOD Assets.

December 7: DPI received source intelligence that the Taliban had placed 8x PPIEDs on a 50 meter stretch of road in XXX village, XXX district, XXX province, approximately 50m south of XXX. The devices were emplaced under the cover of darkness on December 6 and were of the jug type, with victim-operated pressure plates attached. As a result of this intelligence a search operation was commenced. The search team located all eight of the PPIEDs which were detonated in situ.

December 9: Following the kidnapping of a doctor in XXX on December 5, intelligence originating directly from the DPI allowed CF to mount an operation which led to his rescue and a number of insurgents killed during the operation.

December 9: XXX DPI received information detailing a planned Taliban attack on a joint US ISAF/ALP CP, located within the XXX area of XXX district. The DPI officer immediately reported the details to the relevant US ISAF S2 cell, which was immediately fed into the ISAF/ANSF commanders at the CP. As anticipated, ISAF/ALP CP came under small arms fire and underslung grenade launcher rocket attack from multiple firing points. It is assessed by the ISAF S2 cell that due to receiving the threat warning in a timely and accurate manner the joint forces were able to prepare and take up defensive positions within the CP to enable them to react to the attack affectively. As a result there were no casualties.

December 11: XXX DPI received information detailing the location of a recently heavily IED seeded compound within the village of XXX, XXX district, which is located close to a Joint US ISAF/ALP CP and is an area frequently patrolled and visited by the US ISAF/ALP units. Minutes after the information had been passed, another report was received adding that a Joint ISAF/ALP patrol was patrolling towards the compound. XXX DPI immediately reported this to US ISAF S2 cell. As a result of the information relayed to the US ISAF S2 cell, a message was passed to the Joint ISAF/ALP on-ground patrol commanders who conducted a search around the reported compound; as a result there were no casualties and 10x IEDs were located and dealt with.

December 11: Col XXX, the OCC-P commander requested assistance from Legacy as he had no interpreter and was developing a situation with one of his ANSF counterparts. Legacy ACA XXX was briefed by the mentor and the Col and subsequently made contact with an NDS officer who, in turn,

supplied a detailed location of an IED planted near the main highway. An operation was subsequently mounted by the NDS who arrested a suspected Insurgent INS. The INS admitted that he had intended to launch an attack on a large number of ANSF/GIRoA officers as they withdrew their wages. The INS also intended to detonate himself as further ANSF responded to the initial attack. Two mortar rounds to be used as IEDs and a suicide vest were recovered.

December 15: DPI intelligence led to an operation and arrest of a top Insurgent in the XXX district. Further arrests are expected as a result of this intelligence.

December 22: DPI received time sensitive source information that named insurgents had left XXX village to travel to XXX village with intent to ambush ANSF. The ANSF were alerted and were able to successfully engage the insurgents.

December 15: DPI received intelligence from a known source indicating that an IED had been placed on the main road in the village of XXX. An operation resulted in the recovery of a fully primed IED.

December 19: A DPI source stated that Taliban in XXX had placed a red motorcycle VBIED on the main road close to PHQ. An intelligence led search operation by ANP officers discovered and made safe said motorcycle VBIED close to XXX PHQ.

December 20: DPI received source intelligence that insurgents had placed a remote controlled mine on the main road in the village of XXX. An ANP intelligence-led operation successfully discovered and made safe a remote controlled IED constructed from a mine in the village of XXX.

December 23: DPI intelligence indicated that a leading Taliban commander and IED expert was resident in XXX village in XXX district. It was believed this commander had a munitions hide in XXX village containing two remote controls and five detonators. An ANP intelligence-led search operation located and discovered the hide containing the reported two remote controls and a quantity of detonators.

December 23: A DPI team member conducted an emergency telephone debriefing which resulted in the production of a threat warning passed to ANSF and CF; this was followed up with an AIR. The information identified the location of a number of IEDs that had been emplaced during the previous evening in order to target ISAF and ANSF. ANSF deployed to the reported area of the IEDs accompanied by ISAF EOD where they located and detonated 1x RCIED.

December 25: As a result of DPI intelligence that a consignment of drugs was being moved along Highway XXX a joint DPI/ANP operation was mounted at the XXX checkpoint. As a result of the operation a lorry was stopped which was transporting a white minibus on the back. A search of the minibus resulted in 36kg of heroin being discovered. The drugs and the vehicles were taken to PHQ and the driver, who was arrested, handed over to the Counter Narcotics Unit (CNU).

December 25: As a result of DPI intelligence regarding the movement of drugs from Kandahar to Kabul in a specific vehicle the DPI mounted an operation using the XXX checkpoint. A Toyota minibus was stopped and searched and found to contain 7kg of pure opium. Three persons were arrested and taken to PHQ along with the vehicle and the drugs and handed over to the CNU.

May 2013 Examples

April 27: As a result of DPI intelligence a joint operation was mounted in XXX village, XXX district. The operation, which was planned by the DPI, resulted in the following successes; Insurgent Commander 3I/C XXX province and four other insurgents were killed during a gun battle; three injured insurgents escaped the scene, one of whom was later reported dead from injuries sustained. Insurgent weapons were lost as the fleeing insurgents tried to cross the XXX river while in flood. Four motorcycles, one radio and one RPG rocket were seized during the operation.

May 1: As a result of Intelligence received, an operation was mounted by the DPI in the XXX area of XXX, which culminated in the recovery of 10 missiles.

May 2: As a result of intelligence gleaned from XXX the DPI became aware of planned attacks on HWY1 between two villages in XXX district. These actions would involve large numbers of insurgents later the same day. The intelligence was passed to the Provincial Chief of Police (PCoP) with the result that ANP forces were tasked to the area where they subsequently engaged Taliban insurgents at XXX. During the battle one Taliban insurgent was killed and three others injured. There were no ANP casualties. 1x RPG, 960x AK-47 rounds, one rocket and 1x Pakistan ID card were recovered.

May 2: DPI intelligence indicated that a group of Taliban intended to carry out a number of attacks in the area of XXX. The ANP were informed and later that same evening approximately seven Taliban insurgents on motorcycles were engaged in a short gun battle. As a result they were chased from the area – no ANSF causalities were reported on this operation. It is not known if there were any Taliban causalities.

May 3: As a result of MICO 2 intelligence reporting an ANSF cordon and search operation was launched in the vicinity of XXX village in XXX district. The MFT from MICO 2, supporting the 3rd Kandak, reported that the Taliban shadow governor for XXX province, "XXX", along with 20 Taliban fighters from the XXX district, were using the wooded area around XXX village. A joint cordon and search operation was launched into the wooded area of the village and a fire fight ensued. Consequently, four Taliban were killed and three were detained. One RPG rocket launcher, one AKM assault rifle and associated ammunition were recovered.

May 5: Over the last 10 week period the DPI in XXX province has regularly submitted intelligence in relation to the location of approximately 1,500lbs of highly volatile explosive material. During the early

hours of Sunday May 5 Romanian Special Forces from FOB Airborne, supported by American SF, mounted a planned operation in the XXX area to deal with this cache. The explosives were located and neutralized in situ.

May 5: As a result of DPI intelligence received a planned operation took place at XXX village, XXX district, XXX province involving DPI, ALP, ANP and NDS. After firing at Afghan security forces an arrest was made and the suspect was found to be wearing a sophisticated suicide vest. Weapons / explosives seized included the suicide vest and an AK-47 assault rifle.

May 6: Intelligence from XXX district DPI indicated where an IED had been emplaced in the roadway close to XXX village, in XXX district. The ANP authorities were informed and an operation was carried out which successfully located the device. The ANP destroyed the device in situ. There were no arrests in connection with this operation.

May 8: Information supplied by MICO 2 led to several compounds being identified as suspicious in XXX village, XXX district. The Information was passed to 2 Company, 6 Kandak, 2nd Brigade. The Kandak subsequently launched a search operation into the compounds identified by the MICO. In one compound a quantity of explosives and a suicide vest were found.

May 10: Intelligence from XXX DPI indicated that an IED had been emplaced under a drainage bank at the bottom of XXX Hill in the area of XXX, XXX district. The device was located and destroyed following a search operation.

May 15: DPI in XXX received intelligence relating to the location of an IED. The intelligence was disseminated to the DCOP who initiated a follow up search. ANSF conducted the search and located the IED which was destroyed in situ.

May 16: XXX DPI received information indicating the location of two IEDs. This intelligence was disseminated to the DCOP who initiated a follow up search. ANSF conducted the search and located the two IEDs, which were destroyed in situ.

May 16: The DPI and other ANSF conducted an intelligence led operation to intercept a cargo of weapons hidden inside a container and believed to be on route to Kabul via Jalalabad. The container lorry was stopped at the XXX and the driver and passenger found to be dressed in NDS uniforms. On searching the container they discovered equipment and weapons purporting to be from a recently closed FOB in XXX district in XXX province, namely 47x AK-47 assault rifles, 7x PEKA machine guns and military clothing. The persons dressed in NDS uniform were arrested at the scene.

May 18: Information supplied by an MFT from MICO 2 identified the time and location of a possible planned Taliban ambush in the vicinity of XXX village, XXX district, XXX province. 5th Commando Kandak

were tasked to the area and as a result a 10 minute firefight ensued which resulted in one Taliban insurgent killed. The surviving Taliban fled the area.

May 20: Following information received by deployed personnel of 203rd Corps, MICO (3) MFT, one insurgent was detained by the ANA in possession of a primed IED.

May 20: An intelligence-led operation involving XXX DPI resulted in the arrest of a deputy Taliban commander and the identification and safe disposal of four IEDs.

May 21: Intelligence from XXX district DPI indicated the location of a RCIED which had been emplaced in a wall alongside the road one kilometer north of XXX district center. The intelligence indicated that the device was to be used to attack an AUP ranger vehicle which regularly used this route. The ANP authorities were informed and an operation was carried out which successfully located the device. The device was subsequently destroyed in situ.

May 22: The XXX team received information from a source identifying the location of an IED; the team passed the information to the Kandak. The MHT subsequently deployed to the area with an element of the Kandak and recovered the IED. During the search operation the team received further information by telephone from the source; this led the MHT to a compound where they detained an individual suspected of emplacing the IED.

May 23: Intelligence from XXX district DPI indicated the location of an anti-vehicle IED which had been dug into the center of the non-asphalt road in XXX village, XXX district, XXX province. The device was subsequently located and defused by the AUP.

May 23: As a result of DPI source intelligence AUP and ALP officers commenced a search of a given grid location. The search team located a PPIED emplaced at the side of the road. The device was recovered and transported to a local AUP CP for forensic exploitation and destruction by ISAF.

May 24: DPI intelligence led to the discovery of two remote control IEDs which had been placed under a bridge in the vicinity of XXX Road, XXX district, XXX province. The IEDs were made safe by the EOD engineering team from XXX provincial PHQ.

May 27: As a direct result of intelligence received by the DPI an IED was recovered and made safe in the XXX area of XXX district.

May 27: Source intelligence received indicated that approximately 250 Taliban insurgents armed with AK-47s, PKMs, RPG-7s and mortars planned to attack and overrun a series of named ALP, ANP and ANA checkpoints between XXX and XXX, along the XXX valley, effectively cutting off XXX district. As a result, a total of four infantry rifle companies were deployed to the area. The operation disrupted the attack as it

began, with an estimated 100 Insurgents being dispersed. Following an intermittent firefight, lasting almost 12 hours, four insurgents were detained with the only injuries incurred by ANSF being an ANA soldier with GSW to his right hand. Insurgent casualties/fatalities are unknown at this time.

OBSERVATIONS

Over the course of Legacy's delivery we have received feedback from beneficiaries or monitors of the program. A selection of these is provided below.

Observation	Individual, Rank and Organization
5 June 2013 As the troop withdrawal gathers pace the Coalition Forces will become more dependent on such programs [as Legacy] to deliver training and mentoring within the policing arena, with a second order impact of enhancing FOB security and reduce CF and ANSF casualties.	Lt Gen Nicholas Carter, Deputy Commander, ISAF
27 March 2013 I have not seen any better training as proficient or that has provided the level of contributions ... as those provided by Legacy.	Cpt Kemp, SFAT S2 Commanding Officer, FOB Tarin Kot, RC-S
March 2013 [New Century's human intelligence source operations doctrinal-based training] fulfills a US Central Command joint urgent operational needs statement for building Host Nation information and intelligence capacity.	US Government, Combating Terrorism Technical Support Office, 2012 Review
16 March 2013 Please allow me to express my thanks for the fine jobs that the Legacy team has done ... [your personnel] were instrumental in uncovering two threatening individuals ... and their actions may have prevented an attack against my Marines. True professionals and team players, [your personnel] have been a real pleasure to work with.	Cpt Clements, Commanding Officer, operational element, US 9th Marine Regt, RC-SW
23 February 2012 I am proud to have overseen the Legacy program on my watch. There has been a tangible increase of exploitable intelligence directly as a product of the Legacy training. This has resulted in the recovery of; weapons, ammunition, explosives and the arrests of insurgents .... I am leaving Fiaz next week and returning to the USA to brief the new SFA commanders. My recommendation to them is that they continue in the same direction.	Colonel Connor, Commanding Officer, FOB Fiaz, RC-E
9 February 2012 The Legacy program has produced substantial results in RC-S ... under the Legacy training and mentoring programs, the quality and reliability of the [ANSF intelligence] reporting has significantly improved.	Brigadier General Schweitzer, DCG, Operations

New Century
BUILDING INTELLIGENT CAPACITY

Observation	Individual, Rank and Organization
16 September 2011 NCC has been performing admirably. At CTTSO they are looked at as the 'best practices' 'sub'-contractor.	Bryan Taylor, Program Analyst – SETA Contract Support Staff, CTTSO
19 July 2011 ... with regard to the instructors and [surveillance support trainers] in particular, most Coalition trainers find it very difficult to adjust to the way Afghan police officers do business, but the Legacy trainers understand and do it seamlessly.	Colonel Hayatullah, Commandant – ANITC
18 July 2011 Legacy instructors are the best Coalition instructors in Afghanistan, you will not find better anywhere.	Colonel Chester, Divisional Chief MOI – CSTC-A
5 July 2011 Project Legacy continues to demonstrate the ability to rapidly develop security force intelligence capability throughout Afghanistan. Commanding generals across multiple regional commands have recognized the program's contributions towards the ISAF mission and towards the transition to ANSF-led security.	Major General Mallory, DCG – NTM-A / CSTC-A
1 July 2011 This is one of the best observed programs providing tangible capability to ANSF forces.	Counterinsurgency (COIN) Advisory and Assistance teams (CAAT) RC-S inspection report
27 April 2011 The Legacy program possesses an unequalled ability to enable the ANSF police and military intelligence forces to penetrate insurgent and criminal networks ... the Legacy program provides an unmatchable means to provide full-time, in-depth HUMINT training to the ANSF forces.	Major General Toolan, Commander - II MEF (FWD) / RC-SW
6 May 2010 Legacy has demonstrated a ground-breaking approach for rapidly establishing host-nation security force intelligence capacity and capability, first in Iraq and now in Afghanistan. The effects of the Legacy approach are potentially game-changing in Afghanistan.	General McChrystal, Commander – ISAF
January 2010 Th[is] is a superb program which delivers a critical capability to partner nation counterinsurgency forces and valuable collateral benefits to US forces. Legacy is an exceptional program that clearly benefits the overall US counterinsurgency campaigns.	US Government – Commissioned Independent Assessment, LUKOS
27 August 2009 I never realized just how good the training was. The students are totally absorbed by it.	Lieutenant General Helmick, Commander – MNSTC-I / NTM-A

New Century
BUILDING INTELLIGENT CAPACITY

Observation	Individual, Rank and Organization
1 July 2008 Immediately effective.	General John Allen, Deputy Commander – US CENTCOM
24 June 2008 I wanted to thank you again for all your terrific work on our behalf over the last year or so in Anbar and elsewhere. It's making a difference. It's being felt.	General John Allen, Deputy Commander – US CENTCOM

TRANSITION

The proof of a successful program is the eventual autonomous application of the underlying skills, doctrine and processes without the presence of mentors and trainers, coupled with an indigenous ability for host nation personnel to teach the know-how to future generations of intelligence officers / source handlers. Therefore, the desired end state of the Legacy program is to have transitioned ANP DPI and ANA G2 units at the national, provincial, district and local level to this independent, self-sufficient state. To evaluate progress towards this end state, an empirical performance and compliance measurement system, entitled the Professional Standards Transition Model (PSTM), has been designed and introduced by program personnel. This dynamically assesses the competency in the HUMINT capability of units and mentees.

Specifically assigned Performance Compliance Officers (PCOs) inspect every mentoring location on a regular basis in order to evaluate and score the progress of six categories of technical activity in the context of supporting the ANSF HIMINT capability. These are:

- Doctrine – as developed by NC's Technical Department and delivered by the mentors
- Operational command and control and operational deployment
- Materiel – the equipment, apparatus, supplies and security of sites to support the capability
- Personnel – recruitment, retention, training, motivation and personal development
- Training to facilitate the transfer of the HUMINT skills to mentees to enable operational performance to be enhanced and institutionalized
- Relationships, such as those between commanders and their subordinates, and amongst the mentees within their own organizations and with other ANSF bodies.

The PSTM adopts an Aspect Rating Scheme (ARS) which establishes a scoring mechanism for each of the four key attributes of the PSTM measurables, namely:

- People – ability
- Doctrine – proficiency
- Administration – efficiency
- Institutionalization.

Through the application of the ARS to each of the measurables linked to a capability, PCOs collect data that provides an indication on the performance of individual members of the ANSF and the degree of institutionalization within the organization. Aggregate scores are applied across the measurables for each individual capability and a performance score (0 to 5) is attained for that capability. The aggregate scores across all capabilities within each category provide a score for that category.

The model intelligently discriminates between those aspects of the measurables which the Legacy program can control, those which can be influenced, and those over which the program has no control. Each aspect has been tagged using these discriminators within the supporting bespoke software.

In summary, PSTM provides the basis for a multi-dimensional and multi-tiered management tool designed to capture a wide range of data through inspections by PCOs. The model enables an objective determination to be reached as to the readiness of the assessed component of the ANSF organization to transition to independent operation. It does this through analyzing collected data to measure the performance of mentees and ANSF sites, along with the transfer of HUMINT skills and doctrine application. It also facilitates an assessment of the institutionalization of the program through the application of the ARS to the measurable linked to each capability.

Customized software generates a number of valuable reports illustrating, primarily graphically, the state of each assessed ANSF HUMINT component, and its quantifiable compliance with the performance metrics which track its readiness to transition. Process adjustments can be made to the mentoring and training provided, and / or recommended to the relevant ANSF leadership in order to minimize the timeframe to achieve the requisite level of autonomous capability to achieve transition.

We believe that the PSTM is an unique tool and that Legacy is the only capacity-building program which incorporates an integrated, empirical measurement tool to: (1) monitor progress towards the desired end state of a fully transitioned capability; (2) provide empirical feedback to the US Government program managers on performance and progress; and (3) assist project personnel deliver their capacity-building mission and expediently achieve transition.

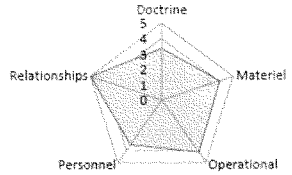
An example of a location transition status report is provided below.

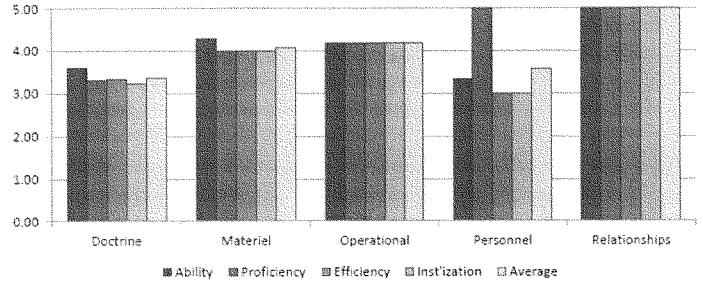
New Century
BUILDING INTELLIGENT CAPACITY

Professional Standards Transition Model: Transition Report (LE)

Executive Summary

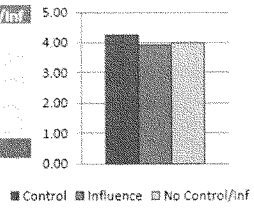
Regional Command	RC(S)
Stream	DPI
Province	Kandahar
District	Kandahar (City)
Unit Name	Kandahar DPI PHQ
Level of Command	PHQ
Visit No	2
Start Date	27-Apr-13
End Date	30-Apr-13
PCO	
PIM	





Category	Ability	Proficiency	Efficiency	Inst'ization	Average
Doctrine	3.62	3.31	3.33	3.23	3.37
Materiel	4.29	4.00	4.00	4.00	4.07
Operational	4.20	4.20	4.20	4.20	4.20
Personnel	3.33	5.00	3.00	3.00	3.58
Relationships	5.00	5.00	5.00	5.00	5.00
Average	4.09	4.30	3.91	3.89	4.05

Category	Control	Influence	No Control/Inf
Doctrine	3.25	3.32	3.00
Materiel	3.86	4.07	4.20
Operational	4.20	4.20	N/A
Personnel	5.00	2.89	3.67
Relationships	5.00	5.00	5.00
Average	4.26	3.89	3.97



New Century
BUILDING INTELLIGENT CAPACITY

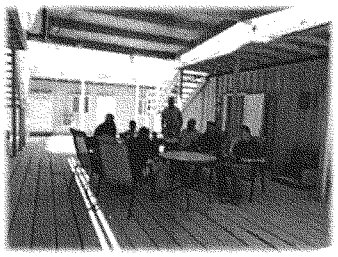
ILLUSTRATIONS

One technique by which we capture a record of the achievements and success of the Legacy program has been the compilation and maintenance of an extensive picture gallery. The photo montage below is an illustration of this.

<table>
<tr><td>Procedures and relationships that exist have resulted in quantitative and qualitative examples of key organizational advances with mentee organizations.</td><td> 
Policy Development with Zone 404 DPI Director</td></tr>
<tr><td> 
Regional Manager of RC-S awarding 'Best DPI BSMC Student' at FOB Walton</td><td>Legacy training delivery and materials has been greatly appreciated by the Afghans and regularly recognized for its quality by CF.</td></tr>
<tr><td>Transition of training to the Afghans developed with excellent cultural awareness of training teams and exemplified by ANSF control of some HUMINT training.</td><td> 
NC and Afghan co-delivery of police training at PITC, Kabul</td></tr>
</table>

New Century
BUILDING INTELLIGENT CAPACITY

Infrastructure, equipment and supplies procured and set up during Legacy have proven to be absolutely fit-for-purpose. Lessons Learned have produced a flexible and enduring approach to the building and transition of HUMINT capability for the ANSF.



Legacy infrastructure at the BAF Compound – includes classrooms, offices, and accommodation

Weapons cache recovered at Kandahar

Legacy is developing an intelligence capability in the ANSF that is effective and increasingly institutionalized in the country. Countless operational successes are greatly indicative of this.

The doctrine has been grounded in the field as a result of our high level of expertise in COIN police and military operations. This expertise is both relevant to Legacy and has endowed our customers – the US Government and ANSF – with a sense of value and confidence.

HUMINT mentor debriefing mentee at FOB Geronimo

New Century
BUILDING INTELLIGENT CAPACITY

FURTHER INFORMATION

A full set of the Operational Successes monthly reports of which examples are set out in the "Successes" section above, and other statistics can be furnished by the Irregular Warfare Support Program at CTTSO. The POC is:

Bryan Taylor — Subject Matter Expert, IWSP
Email — bryan.taylor.ctr@cttso.gov
Telephone — (571) 372-7226

For any further information required of New Century please contact:

Michael Grunberg — Chief Operating Officer
Email — michael.grunberg@newcentcorp.com
Telephone — +44 1481 700 001

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

JUNE 28, 2013

QUESTION SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. In Unisys' experience of integrating biometrics solutions for international customers, what lessons have you seen that might be applied to our own biometrics challenges?

Mr. COHN. See attached.

Supplementary Testimony of Mr. Mark L. Cohn
Vice President, Engineering and Chief Technology Officer
Unisys Federal Systems, Unisys Corporation

Presented to the House Armed Services Committee
Subcommittee on Intelligence, Emerging Threats and Capabilities

August 16, 2013

Chairman Thornberry, Ranking Member Langevin, and other distinguished Members of the Subcommittee, thank you for the opportunity to appear before you on June 28, 2013 to share information on "Past, Present, and Future Irregular Warfare Challenges: Private Sector Perspectives." In the aftermath of the subcommittee hearing, I was invited to provide supplementary material in response to the following question from Ranking Member Langevin.

> In Unisys' experience of integrating biometrics solutions for international customers, what lessons have you seen that might be applied to our own biometrics challenges?

As an information technology industry innovator and leading provider of integrated security solutions many of which incorporate advanced biometric and identity management technologies, Unisys has developed an understanding of the biometrics industry and customer challenges that are relevant to the United States today.

There are three functional areas where biometric technologies are applied widely around the world. The first of these three areas is large-scale store-match-share systems traditionally used for criminal forensics and civil national identification. These systems largely focus on the ability to collect and store the information needed to perform accurate identification (one to many matching) of both known and unknown subjects who may be uncooperative. Major trends for such systems include increasingly large scale (i.e., populations over 100 million), growth of multi-modal collection and matching (e.g., adding iris, facial, palm, and DNA matching services), and adoption of operational models where enrollment and capture are done by contractors independent of the back end matching system integrator. The majority of this supplementary testimony will concentrate on lessons learned implementing large scale identification systems and how platforms, processes, and technologies that have matured over the last two decades enable us to reduce cost and time to deliver while increasing functionality and performance.

The second broad area of applications for biometric technology is access control systems typically used to protect facilities, borders, or computer networks. These systems generally focus on the ability to perform fully automated verification of authorized access for known cooperative subjects and to refuse entry to others. Significant trends for such systems include greater scalability (spanning dozens of locations under a single control system), enterprise integration with centralized identity and human resource management systems, and dramatic grown in the adoption of biometrics to lower operating costs and increase security. Fast reliable response often depends on rapid exchange and dense storage of compact preprocessed biometric templates that are almost always vendor-specific instead of the larger image files used for collection by identification systems and selection of biometric technologies suitable for verification in a specific use case scenario such as hand vein geometry, voice, or keystroke recognition. Applications range from relatively small systems to secure an individual manufacturing or critical infrastructure facility with a biometric to fully integrated architectures protecting overseas nuclear reactors and secure supply chain operations with a multiple overlapping security technologies. Biometrics can scale across large enterprises, prevent fraud, and eliminate impostor threats when compared with traditional credential based systems that rely on controlled distribution of physical badges. For example, a restricted area whose access is controlled by badge and PIN can easily be compromised if an individual's credential is "loaned" to another person; this is prevented when a biometric is used instead. Globally, receptivity to these applications is paralleled by growing consumer acceptance of biometrics for personal convenience in one to one verification scenarios for retail banking, cell phone access, and expedited movement through security access points.

The third broad area of expanded biometrics use is behavior monitoring and intelligence applications emerging from passive collection systems such as public space surveillance. Popular for soccer hooligan detection and urban area street crime prevention, this is increasingly commonplace for customer and adversary identification in commercial settings and we believe will be a growing element in physical security information management systems. These are generally uncontrolled collections reliant on different sensor technologies than the first two functional areas and often include unwitting subjects. Industry developments here obviously have tremendous value in force protection.

Although biometrics as a general topic clearly encompasses all of these functional areas – plus issues associated with system integrity and other security controls, privacy protection, and countermeasures -- there is substantial heterogeneity in the use cases involved, the technologies used, and the general architectural approaches that must be employed. The Department of Defense has requirements that span this full range and is almost uniquely challenged to exploit the potential for biometrics in additional future

areas. Therefore, it may be useful to know that international developments have led to an industry response where we now can speak of a common platform, architecture, and proven toolset to assist in addressing this wide range of challenges coherently and that some leading international organizations are already utilizing.

Let us now return to consider specific lessons learned from experience implementing large scale store-match-share identification systems. Foremost among these is the value of software reuse. Unisys was one of the first companies to realize the potential benefits of software reusability as a means of reducing cost and managing risk, while accelerating the associated time-to-capability delivery. To that end, we embraced Service Oriented Architecture (SOA) and developed our early biometrics projects in the context of a standards-based framework. This framework serves as a foundation in which reusable software components can be easily and rapidly integrated with other third-party software and hardware technologies. With many subsequent successful customer solution deployments, we are now implementing projects with our third-generation reusable framework, that we call the Library of Electronic Identity Artifacts (LEIDA). LEIDA is a framework of reusable identity artifacts that can be readily integrated with a variety of other technologies, (e.g., matching algorithms, hardware platforms, commercial "middleware") to quickly and economically develop and deploy new biometrics solutions that are flexible, secure, and highly scalable.

A second key observation from our experience is that cost-effective scalable biometric identification solutions depend less and less over time on the unique characteristics of a particular biometric matching algorithm and data collection technology such as an individual vendor's fingerprint, facial recognition, or iris matcher and will generally depend more on other technical and architectural characteristics. The reduced criticality of vendor-specific features implemented for individual biometric technologies is because we have been successfully implementing industry-wide cross-vendor interoperability standards for fingerprint in the late 1980's and into the 1990's and face and iris in the last decade, have seen significant improvements in sensor and match processor cost and performance over the same period, and have proven the business case advantages of multi-modal matching and cross-vendor integrations.

Biometric identification systems must still focus much attention on data collection and image capture quality control because input of useable biometric and biographical information is central for both live samples and batch imports; both of which are becoming more routine and standardized as software and hardware vendor dependency declines. The ability to perform matches across modalities (e.g., fingerprint and face or iris) with a multi-modal fusion service is in our view the key to growing system scale with fewer biometric examiners rather than incremental improvement in performance for any one modality.

Beyond tuning the system to perform the appropriate scale biometric identity matching, we often find the elevated program implementation risk, complexity, and implementation challenges generally come from other functional areas such as the need to provide additional services to support identity management workflows and client business rules, the effort and time to customize systems for specific implementations occasionally discovered during or even after system integration, and to generate and manage reports such as watchlists and handle exceptions. The most important feature of the system to reduce risk and save time and money can now be the ability to plug in new logic, configure new interfaces, and to flexibly adjust workflow and system behavior without time-consuming cycles of custom software development and testing.

Accordingly, experience has led the industry to concentrate on delivering mature capabilities so that our clients receive the following benefits (with examples to illustrate how we make that happen):

> **Full Life-Cycle Support:** With a library that includes more than 600 reusable artifacts, we can more quickly automate the entire identity management life cycle, from biometric collection, enrollment, identification, storage, expert examination, and results through credential production and document authentication
>
> **Vendor Independence:** Our framework supports plug-and-play of different vendors' technologies, while minimizing or eliminating the need for code changes. This enables quick and easy integration of preferred COTS hardware or software from multiple vendors.[1] LEIDA is also a proven means of implementing multiple vendors' algorithms within a single modality. Some of this is due to strong promotion of relevant standards.[2]
>
> **Multi-Modal Functionality:** LEIDA provides a repeatable foundation for integrating any combination of fingerprint, face, iris, voice, palm, latent, and signature collection, and fused or single modality matching for identification (1:many), verification (1:1), and watch lists.
>
> **Scalability and Flexibility:** LEIDA uses a flexible and repeatable SOA-based open architecture designed never to limit scalability or performance. Although LEIDA can be deployed to support much larger implementations, current deployments support galleries up to 110 million. These have been fully tested in field deployments and designed to scale to more than 250,000 biometric enrollments per day. It can be deployed centrally as an authoritative source or as a standalone or fully integrated distributed system. It is also flexible enough to be support smaller scale systems and has been used to implement mobile enrollment and matching capabilities on Windows and iOS platforms.
>
> **Speed to Capability:** Although SOA techniques offer comparatively little value when

[1] Examples of vendors whose technologies are integrated within LEIDA include Safran MorphoTrust (formerly L-1 Identity Solutions), Safran MorphoTrak, NEC, Iris ID, Cognitec, Daon, 3M, Hoyos, Oracle, CrossMatch, AOptix, Aware, IBM, WCC Group, and ImageWare Systems

2 LEIDA is compliant with many domain-specific standards, including international standards such as ISO/IEC, BioAPI, CBEFF, and U.S. Government standards such as ANSI/INCITS, EBTS, EFTS, NFIQ, and FBI-certified WSQ.

> they are used to develop one-off custom solutions, they are extremely powerful when the resulting technology is reused across multiple projects or deployments. Many of our 600 reusable artifacts represent individual use cases that support rapid repackaging and deployment with minimal need for development and testing. The reuse of so many already proven artifacts with a repeatable service delivery methodology enables the delivery of complex solutions in a fraction of the time required by traditional custom development. For example, the large Mexico National ID program leveraged the LEIDA artifact library with the system ready for production within 12 months of contract award.

In our international marketplace, the reality is that acquisition cost can trump other factors with customers some times forced to choose to trade cost against delivery speed or risk avoidance, an important or desired element of functionality, and/or targeted run-time performance which may be important to the mission. Therefore, our goal has been to increase affordability during initial standup and reduce long term cost of ownership without compromising schedule, functionality, or performance. We have adopted several strategies. First, we avoid development effort which reduces both cost and time by re-use. Second, our programmatic structured approach for re-use reduces each customer's maintenance costs by integrating mature components already fully tested from earlier engagements to minimize re-work and longer run by sharing costs of improvements over time. As new capabilities are developed and refined, they are added to the framework and are made available for each subsequent client implementation and also are readily available to enhance or extend previous LEIDA deployments. Third, our customers can benefit from algorithm vendor independence through reduced license fees for matchers in each modality through competition and competitive analysis. Last and perhaps most important, when changes are required LEIDA facilitates easy configuration and adapting workflows, business rules, and transaction management, with minimal code change to keep pace with evolving requirements reducing labor support cost and time to respond to new or emerging needs while minimizing the risk of disruptions to integration progress or even worse to ongoing operations by destabilizing the system if already in production.

Beyond these lessons learned about large scale identification systems and integration practices embodied in the Unisys LEIDA framework, our industry and international experience also has brought to us information relevant to the biometrics challenges facing the United States today regarding mobile collection, force protection including capture at a distance, and emerging commercial and consumer uses that can be applied to DoD missions. I discussed each of these in my earlier testimony and would be happy to provide supplementary material on those topics in an appropriate setting if that would be useful.

Thank you again for the opportunity to speak with the subcommittee on these important topics.

○