AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 112–219

INFORMATION SHARING IN THE ERA OF WIKILEAKS: BALANCING SECURITY AND COLLABORATION

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

OF THE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MARCH 10, 2011

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

66–677 PDF WASHINGTON : 2012

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

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000001 Fmt 05011 Sfmt 05011 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE McCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
SCOTT P. BROWN, Massachusetts
JOHN McCAIN, Arizona
RON JOHNSON, Wisconsin
JOHN ENSIGN, Nevada
ROB PORTMAN, Ohio
RAND PAUL, Kentucky

MICHAEL L. ALEXANDER, *Staff Director*
CHRISTIAN J. BECKNER, *Associate Staff Director for Homeland Security Prevention and Protection*
JEFFREY E. GREENE, *Senior Counsel*
NICHOLAS A. ROSSI, *Minority Staff Director*
BRENDAN P. SHIELDS, *Minority Director of Homeland Security Policy*
LUKE P. BELLOCCHI, *Minority Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk and GPO Detailee*
LAURA W. KILBRIDE, *Hearing Clerk*

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000002 Fmt 05904 Sfmt 05904 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

CONTENTS

	Page
Opening statements:	
Senator Lieberman	1
Senator Collins	3
Senator Brown	14
Prepared statements:	
Senator Lieberman	29
Senator Collins	31

WITNESSES

THURSDAY, MARCH 10, 2011

Hon. Patrick F. Kennedy, Under Secretary for Management, U.S. Department of State	4
Teresa M. Takai, Chief Information Officer and Acting Assistant Secretary for Networks and Information Integration, U.S. Department of Defense, and Thomas A. Ferguson, Principal Deputy Under Secretary for Intelligence, U.S. Department of Defense	7
Corin R. Stone, Intelligence Community Information Sharing Executive, Office of the Director of National Intelligence	9
Kshemendra Paul, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence	11

ALPHABETICAL LIST OF WITNESSES

Ferguson, Thomas A.:	
Testimony	7
Joint prepared statement with Teresa Takai	44
Kennedy, Hon. Patrick F.:	
Testimony	4
Prepared statement	33
Paul, Kshemendra:	
Testimony	11
Prepared statement	59
Stone, Corin R.:	
Testimony	9
Prepared statement	52
Takai, Teresa M.:	
Testimony	7
Joint prepared statement with Thomas Ferguson	44

APPENDIX

Thomas E. McNamara, Former Program Manager of the Information Sharing Environment at the Office of the Director of National Intelligence, prepared statement	68
Markle Task Force on National Security in the Information Age, prepared statement	72
Responses to post-hearing questions for the Record from:	
Mr. Kennedy	81
Ms. Takai and Mr. Ferguson	86
Ms. Stone	102
Mr. Paul	105

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000003 Fmt 05904 Sfmt 05904 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

INFORMATION SHARING IN THE ERA OF WIKILEAKS: BALANCING SECURITY AND COLLABORATION

THURSDAY, MARCH 10, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 3:06 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Collins, and Brown.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good afternoon and thanks for your patience. We just were able to, Senator Collins and I, vote early. And I want to apologize in advance. I am going to have to step out for about 15 minutes in about a half-hour, but I shall return.

In just 6 months and a day, we will mark the 10th anniversary of the attacks of September 11, 2001, and we will honor the memory of the nearly 3,000 people who were murdered that day in America.

Our mourning over their deaths has always been compounded by the knowledge that those attacks might have been prevented—certainly that was the implication of the 9/11 Commission Report—had our intelligence and law enforcement agencies shared the disparate facts they had gathered, enabling us to connect the dots.

To prevent this from happening again, Congress passed several laws intended to strengthen information sharing among critical Federal agencies. Those acts included the Homeland Security Act, the Intelligence Reform and Terrorism Prevention Act (IRTPA), and the USA PATRIOT Act.

Since then, the Executive Branch, I think, has made significant improvements in its information-sharing systems, and there is no question that far more information is now available to partners in other agencies who have a legitimate need for it.

All this intelligence is further brought together at key nodes, such as the National Counterterrorism Center (NCTC), where it can be examined by intelligence specialists from a variety of agencies working together under one roof. And as a result, we have seen a number of successes in recent domestic and military counterter-

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000005 Fmt 06633 Sfmt 06633 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

rorism operations that I think were thanks to that kind of information sharing, and I am going to cite some examples in a moment.

But this Committee's recent report on the Fort Hood attack shows that information sharing within and across agencies is nonetheless still not all it should be, and that allowed in that case a "ticking time bomb," namely Major Nidal Hasan, now accused of killing 13 and wounding 32 others at Fort Hood, to radicalize right under the noses of the Department of Defense (DOD) and the Federal Bureau of Investigation (FBI). So we need to continue improving our information-sharing strategies.

Now I fear the WikiLeaks case has become a rallying cry for an overreaction for those who would take us back to the days before September 11, 2001, when information was considered the property of the agency that developed it and was not to be shared.

The bulk of the information illegally taken and given to WikiLeaks would not have been available had that information not been on a shared system, so the critics of information sharing argue.

But to me this is putting an axe to a problem that requires a scalpel and misunderstands what happened in the WikiLeaks case and I think misstates the solution to the problem. We can and must prevent another WikiLeaks without also enabling Federal agencies, in fact, perhaps compelling Federal agencies to reverse course and return to the pre-September 11, 2001, culture of hoarding information.

We need to be smarter about how information is shared and appropriately balance security concerns with the legitimate needs of the users of different types of information. Methods and technologies for doing so already exist. Some of them I gather have been put into place since the WikiLeaks case, and we need to make sure that we utilize them as fully as possible across our government.

The bottom line is we cannot walk away from the progress we have made that has saved lives. I will give you a couple of quick examples.

U.S. Special Forces and elements of the intelligence community have shared information and worked exceptionally well together in war zones to combat and disrupt terrorist groups such as al-Qaeda in Iraq and the Taliban in Afghanistan. And that would not happen without information sharing.

Here at home, we have used information sharing to enhance the role of State, local, tribal, and private sector entities in our fight against terrorists. And those efforts have paid off—most recently in the case of a chemical supply company in North Carolina that alerted the FBI to suspicious purchases by a Saudi Arabian student in Texas who turned out to be building improvised explosive devices.

So we need to fix what is broken without going backwards. Today I look forward to hearing from each of our witnesses about what they are planning to do to improve the security of classified networks and information, while still ensuring that information is shared effectively in the interest of our Nation's security.

I would also like to hear how Congress can work with you on these efforts either with legislation or through more targeted fund-

ing. Efficiently sharing classified information while effectively securing that information is critical to our Nation's security and our national values. We can and must have both.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Effective information sharing among Federal law enforcement and civilian and military intelligence agencies is critical to our security. The 9/11 Commission found that the failure to share information across the government crippled efforts to detect and potentially prevent the attacks on September 11, 2001. Improving this communication was a critical part of the Intelligence Reform and Terrorism Prevention Act that Senator Lieberman and I authored in 2004.

The WikiLeaks breach should not prompt a knee-jerk reaction on the sharing of vital information and its use by those analysts who need it to do their jobs. We must not let the astonishing lack of management and technical controls that allowed a private in the army to allegedly steal some 260,000 classified State Department cables and some 90,000 intelligence reports to send us back to the days before September 11, 2001.

Unfortunately, we continue to see agency cultures that resist sharing information and coordination with their law enforcement and the intelligence counterparts. Almost 10 years after September 11, 2001, we still witness mistakes and intelligence oversights reminiscent of criticisms predating our reforms of the intelligence community. Among those cases where the dots were not connected and information was not effectively shared are Abdulmutallab, the so-called Christmas Day bomber, and Nidal Hasan, the Fort Hood shooter.

At the same time, as the Chairman has pointed out, there have been several cases that underscore the incredible value and benefit of information sharing, and an example is, as the Chairman has noted, the case of Mr. Zazi, whose plans to bomb the New York City subway system were thwarted.

As such successes remind us, we must not allow the WikiLeaks damage to be magnified twofold. Already the content of the cables may have compromised our national security. There have been news reports describing the disclosure of these communications as having a chilling effect on our relationships with some of our closest allies. More important, however, they likely have put at risk some of the lives of citizens, soldiers, and partners.

Longer lasting damage could occur if we allow a culture to reemerge in which each intelligence entity views itself as a separate enterprise within the U.S. counterterrorism structure, with each attempting to protect what it considers to be its own intellectual property by not sharing it with other counterterrorism agencies. If those stovepipes reappear or worsen, we will certainly be in more danger.

Such a step backward would run counter to the policy goals embodied in the 2004 Intelligence Reform Act, articulated by law enforcement and the intelligence community leadership, and underscored in multiple hearings before this Committee; and, that is, to

effectively detect and thwart terrorists, the "need to share" must replace the "need to know."

I would also like to hear today about the possible technological solutions to the problems that allowed for the disclosures to WikiLeaks. For example, my credit card company can detect out-of-the-ordinary charges on my account almost instantaneously. Yet the military and intelligence communities were apparently unable to detect more than a quarter million document downloads in less than 2 months. Surely, the government can make better use of the technology currently employed by the financial services industry.

It is also notable that the intelligence community was already required to install some audit capabilities in its systems by the 2007 homeland security law, which we authored, that could well have included alerts to supervisors of suspicious download activity. Had this kind of security measure been in place, security officers might have detected these massive downloads before they were passed on to WikiLeaks.

Technology and innovation ultimately should help protect information from unauthorized disclosure, while facilitating the appropriate sharing of vital data.

I would also like to explore today the implementation of role-based access to secure classified information. Instead of making all information available to anyone who has access to a classified system, under this model, information is made available in a targeted manner based on individuals' positions and the topics for which they are responsible. Access to information not directly relevant to an individual's position or responsibilities would require the approval of a supervisor.

We must craft security solutions for the 21st Century and beyond. We live in a world of Twitter and instantly viral videos on YouTube. We must strive to strike the appropriate balance that protects classified and sensitive information while ensuring the effective sharing of vital data. We can use the most cutting edge technology to protect the traditional tools of statecraft and intelligence—those tools of relationships and information.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins, for that thoughtful opening statement.

I want to thank the witnesses who are before us for coming, also for the thoughtful written testimony you have submitted to the Committee, which will, without objection, be included as part of the record.

Now we will begin with Patrick Kennedy, who is Under Secretary for Management at the Department of State. Welcome, Mr. Kennedy.

TESTIMONY OF HON. PATRICK F. KENNEDY,[1] UNDER SECRETARY FOR MANAGEMENT, U.S. DEPARTMENT OF STATE

Mr. KENNEDY. Thank you very much. Chairman Lieberman, Ranking Member Collins, and Senator Brown, thank you for this opportunity to address information sharing after WikiLeaks and to discuss Executive Branch efforts to ensure that information is

[1] The prepared statement of Mr. Kennedy appears in the Appendix on page 33.

shared effectively yet securely and in a manner that continues to advance our national security. The State Department and our interagency partners have long been working to obtain both appropriate information sharing and protection, and after WikiLeaks, we have focused renewed attention on achieving these dual objectives.

From my perspective, serving over 30 years with the State Department, both overseas and in Washington, and also serving as the first Deputy Director of National Intelligence for Management, I especially appreciate your efforts to address with us the challenges of information sharing and security. I can assure you that we at the State Department remain committed to fully sharing our diplomatic reporting within the interagency with safeguards that are reasonable, pragmatic,and responsible.

For diplomatic reporting, the State Department has historically communicated between Washington and overseas posts through messages which convey internal deliberations relating to our foreign relations and candid assessments of overseas conditions. This reporting provides the State Department and other U.S. Government agencies crucial information essential to advancing our national interests, and we continue to this day to share this reporting through automatic dissemination to over 65 U.S. Government agencies.

In late November 2010, when the press and WikiLeaks announced the release of purported State Department cables, we immediately established a 24/7 WikiLeaks Working Group of senior State Department employees; we did suspend the Secret Internet Protocol Router Network (SIPRNet) to Net Centric Diplomacy, the database of State Department cables, while retaining all of our other distribution systems to other agencies. We also created a mitigation team to address policy, legal, and counterintelligence issues.

For continued mitigation efforts, both within the State Department and interagency, we continue to deploy an automated tool that monitors State's classified network to detect anomalies not otherwise apparent, backed up by a staff who analyze these anomalies. Cable distribution has been limited to the Joint Worldwide Intelligence Communications System and our traditional system that reaches out, as I said, to 65 agencies. We are now evaluating other systems for distribution, such as a searchable database that relies on metadata.

The State Department has continued to work with information management issues interagency through the Interagency Policy Committee (IPC), chaired by the White House's Special Adviser for Information Access and Security, as well as through existing IPCs.

The challenges of grappling with the complexities are threefold.

The first is ensuring information-sharing policies are consistently directing the use of technology to solve problems, not the other way around. Post-September 11, 2001, the focus was on providing technical solutions to information sharing. As a result, technical experts were asked to develop solutions to the barriers. The post-WikiLeaks environment reminds us that technology is a tool to execute solutions but it is not in itself the answer. Simply put, we must more consistently sort out what we need to share before determining how to share it. Connecting systems and networks may

provide the means to share information, but we must still manage and share this content in an effective and efficient way, as both of you mentioned in your opening statements.

The national security community must do a better job of articulating what information is appropriate to share with the widest appropriate distribution and what is more appropriately confined to a narrower audience across the community in order to ensure adequate safeguards. The State Department believes that the way in which we share messages through our traditional means of dissemination and the steps we have taken since November are leading us firmly in that direction.

The second main challenge involves each agency's rigorous adherence to existing and improved information security policies, as both of you have noted. This includes improved training in the use of labels to indicate appropriate breadth of dissemination. The Executive Order on classified information establishes the basic levels of classification. From that foundation, individual agencies may still have their own captions that denote how information should be disseminated because obviously not every person with a security clearance needs every piece of worldwide information. Agencies that receive information need to understand how to handle that captioned information so that it is not inappropriately made available to too wide an audience.

The Office of Management and Budget (OMB) has directed agencies to address security, counterintelligence, and information issues through special teams. We believe that our Mitigation Team serves as a model for broad, cross-discipline coordination, or governance because it brings together the various subject matter experts. Many information-sharing and security issues can be resolved at the agency level as long as there are standards in place for agencies to execute. For the most part, standards have been created by existing interagency bodies, but there are some areas where further coordination is needed.

The third main challenge involves the coordination, or governance, of information management. Numerous interagency groups are wrestling with the issues related to technological aspects of information sharing, such as those dealing with standards, data standards, systems, and networks. Others are wrestling with the policy decisions of who should have access to what information. New interagency governance structures to coordinate information sharing have been developed, including those focused, as you rightly note, on sharing with State, local, and tribal governments, as well as with foreign partners. In keeping with the first challenge, these new structures should maintain or increase focus on defining the content to be shared and protected as well as on the technology which is to be shared and used. Each agency must be confident that security processes and procedures are applied in a uniform and consistent manner in other organizations. And, in addition, it must be understood that material originating in one agency will be treated by other agencies in accordance with mutually understood handling instructions.

The State Department shares information with the intent of providing the right people with the right information at the right time. We will continue to share our diplomatic reporting in order to ad-

vance our national security information. We recognize the imperative to make diplomatic reporting and analysis available throughout the entire interagency community. The State Department will continue to do this in order to fulfill our mission.

We remain committed to both appropriately sharing and protecting critical national security information, but this commitment requires, as you have noted, addressing multiple, complex issues. We must find the right policies; we must find the right technologies; and we must continue to share.

Thank you for this opportunity to appear before you today. I look forward to working with you on the challenges and would be pleased at the right time to respond to any questions you might have. Thank you.

Chairman LIEBERMAN. Thanks very much, Secretary Kennedy.

Now we are going to hear from Teresa Takai, Acting Assistant Secretary for Networks and Information Integration, Chief Information Officer, U.S. Department of Defense. Welcome.

TESTIMONY OF TERESA M. TAKAI,[1] CHIEF INFORMATION OFFICER AND ACTING ASSISTANT SECRETARY FOR NETWORKS AND INFORMATION INTEGRATION, U.S. DEPARTMENT OF DEFENSE, AND THOMAS A. FERGUSON, PRINCIPAL DEPUTY UNDER SECRETARY FOR INTELLIGENCE, U.S. DEPARTMENT OF DEFENSE

Ms. TAKAI. Thank you, sir. Thank you for that introduction. Chairman Lieberman, Ranking Member Collins, and Senator Brown, thank you for the invitation to provide testimony on what the Department of Defense is doing to improve the security of its classified networks while ensuring that information is shared effectively.

As noted, I am Teri Takai, and I serve as the principal adviser to the Secretary of Defense for Information Management, Information Technology, and Information Assurance, and as such am responsible for the security of the Department's networks and then coordinating the Department's mitigation efforts in response to the WikiLeaks incident.

With me is Tom Ferguson, Principal Deputy Under Secretary for Intelligence. He serves as the principal staff adviser to the Under Secretary of Defense for Intelligence and is responsible for policy and strategic oversight of all DOD intelligence, counterintelligence, and security policy, plans, and programs, as delegated by the Under Secretary for Intelligence. In this capacity, Mr. Ferguson oversees the development and implementation of the Department's information-sharing policies.

Mr. Ferguson and I have submitted a detailed statement for the record, but I would like to briefly highlight a few of the Department's efforts to better protect its sensitive and classified networks and information while ensuring its ability to share critical information with other partners and agencies is continued.

Immediately following the first release of documents on the WikiLeaks Web site, the Secretary of Defense commissioned two in-

[1] The joint prepared statement of Ms. Takai and Mr. Ferguson appears in the Appendix on page 44.

ternal DOD studies. The first study directed a review of DOD information security policy. The second study focused on procedures for handling classified information in forward-deployed areas. Results of the two studies revealed a number of findings, notably that: Forward-deployed units maintained an overreliance on removable electronic storage media; second, roles and responsibilities for detecting and dealing with an insider threat needed to be better defined; and, finally, limited capability existed to detect and monitor anomalous behavior on classified computer networks.

The Department immediately began working to address the findings and improve its overall security posture to mitigate the possibility of another similar type of disclosure. The most expedient remedy for the vulnerability that led to WikiLeaks was to prevent the ability to remove large amounts of data from the Department's secret classified network using removable media, such as discs, while allowing a small number of computers to retain, under strict controls, the ability to write removable media for operational reasons. The Department has completed disabling the write capability on all of its SIPRNet machines except for approximately 12 percent that maintain that capability for operational reasons, largely in deployed areas of operation. The machines that maintain write capability are enabled under strict controls, such as using designated kiosks with two-person controls.

We are also working actively with National Counterintelligence Executive on its efforts to establish an information technology insider detection capability and an Insider Threat program. Mr. Ferguson's organization is leading that effort for the Department of Defense, and they have been developing comprehensive policy for a DOD Counterintelligence Insider Threat Program.

In addition, DOD is developing Web-enabled information security training that will complement DOD's mandatory annual information assurance training, and the Joint Staff is establishing an oversight program that will include inspection of forward-deployed areas.

As DOD continues efforts to improve our information-sharing capabilities, we will strive to implement the mechanisms necessary to protect the intelligence information without reverting back to pre-September 11, 2001, stovepipes. DOD is working closely with its interagency partners, several of whom join me here today, to improve intelligence information sharing across the government while ensuring the appropriate protection and safeguards are in place.

I would like to conclude by emphasizing that the Department continues to work towards a resilient information-sharing environment that is secure through both technological solutions and comprehensive policies. Mr. Ferguson and I thank the Committee for the opportunity to appear before you today, and we look forward to answering your questions.

Senator COLLINS [presiding]. Thank you.

Mr. Ferguson, I am told that you do not have a prepared statement. Is that correct?

Mr. FERGUSON. That is correct. Ms. Takai has a nicer voice than I do and has given our joint statement.

Senator COLLINS. Thank you.

Before I turn to our next witness, we have been joined by Senator Brown, and I just wanted to give him an opportunity for an opening statement if you would like to have one.

Senator BROWN. Thank you. I am actually eager to hear from the witnesses and ask questions, but thank you for the offer.

Senator COLLINS. Thank you. Then we will proceed.

Our next witness is Corin Stone, who is the Intelligence Community Information Sharing Executive from the Office of the Director of National Intelligence (ODNI). We welcome you. Please proceed with your testimony.

TESTIMONY OF CORIN R. STONE,[1] INTELLIGENCE COMMUNITY INFORMATION SHARING EXECUTIVE, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Ms. STONE. Thank you, ma'am. Chairman Lieberman, Ranking Member Collins, and Senator Brown, thank you for inviting me to appear before you today to discuss the intelligence community's progress and challenges in information sharing. I want to first recognize the Committee's leadership on these important issues and thank you for your continued support as we address the many questions associated with the need to share information and the need to protect it. Your leadership and oversight of information sharing, especially as we come up to the 10-year anniversary of September 11, 2001, has been invaluable. I look forward to our continued participation and partnership on this complex and vitally important issue.

As the Intelligence Community Information Sharing Executive, I am the Director's focal point for all intelligence community information-sharing matters, providing guidance, oversight, and direction on information-sharing priorities and initiatives across the community. In that capacity, I work in coordination with my colleagues at the table and across the community on comprehensive and strategic management information sharing, both internally and with all of our mission partners.

My main focus today concerns information that is derived from intelligence sources and methods or information that is reflected in the analytic judgments and assessments that the intelligence community produces. I want to be clear, though, that our concern for the protection of information is not only narrowly focused on sources and methods.

As we have seen recently through WikiLeaks, the unauthorized disclosure of classified information has serious implications for the policy and operational aspects of national security. We all have networks that must be secured, and as technology continues to advance, my colleagues and I remain deeply committed to keeping up with the ongoing challenges we face.

I am acutely aware that our major task is to find what the Director of National Intelligence (DNI) has termed "the sweet spot" between the two critical imperatives of sharing and protecting information. Every day our officers work tirelessly to tackle challenges of increasing complexity in a world that is interconnected, fast-paced, and ever changing, sharing vital information with each

[1] The prepared statement of Ms. Stone appears in the Appendix on page 52.

other, customers and partners, leading to better prepared senior policymakers across the Executive Branch and Congress.

It is important to note that the community's work on these complicated questions predates the recent unauthorized disclosures by WikiLeaks. As you know, the challenges associated with both sharing and protecting intelligence are not new and have been the subject of major effort in the intelligence community for years. However, these latest unauthorized disclosures underscore the importance of our ongoing and comprehensive efforts to address these evolving challenges.

Working with the whole of government to address these issues, the intelligence community's strategy involves three interlocking elements.

The first is access, ensuring that the right people can discover and have access to the networks and information they need to perform their duties, but not to information that they do not need.

The second element is technical protection, technically limiting the ability to misappropriate, manipulate, or transfer data, especially in large quantities.

And the third area is auditing and monitoring, taking actions to give the intelligence community day-to-day confidence that the information access granted to our personnel is being properly used.

As we work to both share and protect networks and information, we must never lose sight of the sweet spot. As we continue to increase how much information is shared, we must also increase the protections in place to ensure information is being properly used and safeguarded. This is the only way to create the necessary trust and confidence in our systems that will foster appropriate information sharing. It is a matter of managing risk, and people, policies, processes, and technology all play important interconnected roles in managing that risk.

However, it is also important to note that while all of our capabilities can reduce the likelihood and impact of unauthorized disclosures, in the final analysis our system is based on trust—trust in the individuals who have access to classified information and trust that they will be responsible stewards of this Nation's most sensitive information.

Whether classified information is acquired by a computer system, a classified document, or simply heard in a briefing or a meeting, we have had bad apples who have misused this information before, and we will, unfortunately, have them again. This reality does not mean we should err on the side of not sharing; rather, we must put all proper safeguards in place, continue to be forward leaning to find a threat before disclosures occur, be mindful of the risks, and manage those risks with the utmost diligence.

Thank you for the Committee's time, and I welcome your questions.

Senator COLLINS. Thank you.

Our final witness on the panel this afternoon is Kshemendra Paul, who is the Program Manager for Information Sharing Environment of the Office of the Director of National Intelligence. Welcome, Mr. Paul.

TESTIMONY OF KSHEMENDRA PAUL,[1] PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. PAUL. Thank you, Chairman Lieberman, Ranking Member Collins, and Senator Brown. Thank you for the opportunity to speak about our efforts to effectively share and protect information at every level of government. Thank you for your attention to information-sharing reform efforts and your support of my office's mission. I also want to recognize my fellow panelists, key partners in government-wide efforts to further strengthen information sharing and protection.

As the WikiLeaks story emerged, concerns were voiced that the information-sharing efforts would suffer a setback. This Administration is committed to strengthening both information sharing and information protection. While complex and challenging, we do not see these goals as conflicting. Guidance throughout the Executive Branch has been consistent. We need to accelerate information sharing in a responsible and secure way.

The WikiLeaks breach is not principally about information-sharing challenges. A bad actor allegedly violated the trust placed in him. While we cannot always stop bad actors, we can and must take this opportunity to reassess our posture, our progress, and our focus related to improving and strengthening information sharing and protection.

The challenges highlighted by the WikiLeaks breach are complex and go to deeply rooted issues: First, the perpetuation of agency-based, bilateral, and fragmented solutions versus common and comprehensive approaches to information sharing and protection; second, the need to improve our counterintelligence posture and some of the other technical considerations that my fellow panelists have talked to; and, finally, while the breach involves classified information, we need to be mindful that the root cause issues and the sensitivities extend to sensitive but unclassified information also. It is a whole-of-government problem, not just a classified national security problem.

I would like to clarify the information-sharing environment and my role. The purpose of the information-sharing environment is to improve the sharing of terrorism-, homeland security-, and weapons of mass destruction-related information across Federal, State, local, and tribal agencies and with our partners in the private sector and internationally.

The information-sharing environment spans five communities: Defense, intelligence, homeland security, law enforcement, and foreign affairs. It is defined as a cross-cutting, horizontal, data-centric, trusted information-sharing and protection capability. My role is to plan for and oversee the agency-based buildout, and manage the information-sharing environment. But my office is not operational. Agencies own the mission, agencies set policies and procedures, and agencies make the investments that interconnect our networks, databases, applications, and business processes. These agency-based contributions together form the information-sharing environment.

[1] The prepared statement of Mr. Paul appears in the Appendix on page 59.

The law grants the program manager's role governmentwide authority. This authority is exercised primarily two ways: First, I am the co-chair of the White House's Information Sharing and Access Interagency Policy Committee; through that role, we work through policy and oversight issues; and, second, through my partnership with the Office of Management and Budget.

We are being deliberate and collaborative in our approach to further strengthening information sharing and protection. We have put an emphasis on governance and outreach. My office, together with my mission partners, is leading the refresh of the 2007 National Strategy for Information Sharing. We are using this opportunity to leverage common mission equities to drive common policies and capabilities. And we are orchestrating specific agency-led sharing and protection initiatives with our partners.

We believe this work provides a framework for strengthening efforts to address the root cause issues associated with the WikiLeaks breach. These capabilities will result in further assuring the proper sharing and protection of information.

Our work across mission partners is profiled in our annual report to the Congress delivered every summer. I also encourage those interested in following or influencing our efforts to visit our Web site and to participate in upcoming online dialogues aimed at shaping our future direction.

In closing, our efforts have been and continue to be focused on accelerating information sharing in a secure and responsible way. Effective information sharing and collaboration are absolutely essential to keeping the American people safe.

Thank you for the opportunity to participate in this hearing. I also would appreciate any comments, directions, support, or feedback that you can provide to me in my office. My fellow panelists and I look forward to your questions.

Senator COLLINS. Thank you very much for your testimony, and I thank all of the witnesses.

I want to express my personal frustration with this issue. Our Committee has held hearings on the lack of information sharing in the case of Abdulmutallab, where credible information was given to our embassy in Africa but did not make its way in a timely fashion to the National Counterterrorism Center and, thus, Abdulmutallab was not listed on the No Fly List. So there is an example of credible information that should have been shared across government but was not.

Similarly, in our investigation into the Fort Hood attacks, we found that credible information about Major Hasan's communications with a known terrorist suspect was not shared by the Joint Terrorism Task Force with the Army—another terrible failure in information sharing.

Now, there have been successes as well. But I mention those two failures to contrast and raise such questions with how an Army private allegedly was able to download hundreds of thousands of classified documents, cables, and intelligence reports without being detected, and that baffles me. It also frustrates me because in 2007, Senator Lieberman and I authored homeland security legislation that included a requirement that military and intelligence agencies install audit capabilities with robust access controls on

classified systems. And those technologies that would enable us to audit information transmission and authenticate identities for access control are not new. They are widely used. And the serious cyber risks associated with the use of removable media devices, such as thumb drives, have been known for many years.

How did this happen? How could it be that a low-level member of the military could download such a volume of documents without it being detected for so long? That truly baffles me. I do not know who to start with. Mr. Ferguson, do you want to take a crack at that?

Mr. FERGUSON. I will be the first in the pond. Let me take it in a couple steps. Your question has a lot of parts to it.

The rank of Private Bradley Manning is really not so much the issue. It was what his responsibilities were. He was there to provide intelligence support for military operations. So we do not base it necessarily on a rank structure. We base it on what is his mission responsibilities to support the military.

To get to your question about how was he able to access so much data, and then I will get to the part about what have we done and why didn't we do what we could have done. The situation in the theater is such that—or was. It has changed now. But we took a risk, essentially is what it is. We took a risk that by putting the information out there, share information, provide agility, flexibility of the military forces, they would be able to reach into any of the databases on SIPRNet. They would be able to download that information, and they would be able to move the information using removable media across various domains, whether it is across security domains or from U.S. systems to coalition systems. And we did that so they could do this very rapidly.

Here in the Continental United States (CONUS) many of the things you have talked about, about closing off open media ports and so forth, actually have been in place for a decade or more. If you go to many of the agencies, they actually are not able to access those open ports. But the focus in the theater was speed and agility, so we took that risk to allow not just Private Manning but many people who are serving there to move at that pace.

You asked about why we did not put in place capabilities that were in your bill. In fact, as early as 2008, we started to deploy what is called the Host Based Security System (HBSS), as early as 2008. And at the time of Private Manning's alleged activities, about 40 percent of the systems in CONUS actually had that system in place. The systems were not—that was not available in the theater.

Senator COLLINS. And why wasn't it?

Mr. FERGUSON. Mainly because of a lot of the systems there are, for lack of a technical term, cobbled together, and placing those kinds of systems—they are not all equal. It is sort of a family of systems there, and it is not just like working for Bank of America where they have one homogeneous system and they can insert things and take things out as it works. You have multiple systems and putting in new intrusion software or monitoring tools and so forth, you have to approach each system differently. And that is part of the problem.

So basically to get away from that and not hold up the ability to move information, they took on the risk by saying, look, these

people are cleared. They go through background investigations, and, frankly, most of our focus was right about outside intruder threat, not inside threat.

So in the end, to answer your questions—we had ourselves a situation where we had information sharing at this level, and we took the risk of having monitoring tools and guards and passwords and so forth, as well as people did not fully implement policies, they did not follow security rules down at this level. So the problem is that is where we made our mistake. We allowed this to occur when we were sharing information at this level. So what we are trying to fix today is not take this level of information sharing and moving it down here, which you have referred to in your opening statement, but take this and move it up here. And that is what we are trying to do as rapidly as we can.

Senator COLLINS. Thank you.

Mr. Kennedy, Mr. Ferguson basically explained that DOD, in the interest of making sure that the information was out there in theater, took a risk, but that does not explain to me how the private would have access to State Department classified cables that had nothing to do with the country for which the private was involved in intelligence activities. So how did it happen that he had access to classified State Department cables, involving countries that had nothing to do with his intelligence responsibilities?

Mr. KENNEDY. That is a very good question, Senator. Several years ago, the Department of Defense and the intelligence community came to the State Department and said, we need the State Department—and actually they paid for it—to push out reporting to SIPRNet, which is the Department of Defense worldwide system, and to load a number of our cables onto a Defense Department database that would be accessible to Defense Department people. So in response to their request, we took a selected element of our cables and pushed those out to the Department of Defense's database.

To be blunt, we believe in the interest of information sharing that it would be a grave mistake and a danger to the national security for the State Department to try to define in each and every one of the 65 agencies that we share our diplomatic reporting analysis with to say that Private Smith should get this cable, Lieutenant Jones should get that cable, Commander X should get that cable. The policies that have been in place between the State Department and other agencies is we provide this information to the other agency. The other agency then takes on the responsibility of controlling access by their people to the material that we provide to them.

Senator COLLINS. I will come back to that issue, but I want to first give an opportunity for my colleague, Senator Brown, to ask his questions.

OPENING STATEMENT OF SENATOR BROWN

Senator BROWN. Thank you. You are on a roll, though.

I have served in the National Guard for 31 years. I am a Lieutenant Colonel. I am on the computers regularly, all that good stuff, and I have to tell you, sometimes it is like brain surgery getting on the computer, even for somebody like me who is part of the

senior staff, and had been a trial defense attorney, just to log on, get access, go where I need to go, and I still have not really gotten a satisfactory answer as to how this private had complete and total access to the documents he had. In my wildest dreams, I could not do what he did.

And then I see, he works 14 hours a day, no one cares. Well, the average workload in that region is that and more for many people.

My understanding, in doing my own due diligence, is that there was a complete breakdown of command authority when it came to instructing that soldier and people within that command as to the do's and do not's with regard to information and information sharing. There was no check or balance, and that the amount of people that have access to that information has grown by tens of thousands. Hundreds of thousands of people have access to that information on any given day.

Is that accurate, that that many people have access to that information? Whoever feels qualified to answer it, probably the DOD folks.

Mr. FERGUSON. Let me put it this way: The SIPRNet is a command and control network, just like the Internet.

Senator BROWN. I know what that is, I am in the military. Can you explain to the listeners what that is?

Mr. FERGUSON. What is the SIPRNet?

Senator BROWN. Yes.

Mr. FERGUSON. The SIPRNet is a command and control network that maintains Department of Defense classified secret level information that covers a whole portfolio of issues. It is not just intelligence information, for one. It is operations data. It is financial programmatic data, personnel data. It covers a very large——

Senator BROWN. It is everything.

Mr. FERGUSON. It is everything. All that information is not available to everyone who is on SIPRNet. A lot of that information, in fact, is password protected. But there are sites, just like going on the Internet, that if you click on there, if you put in the search for that information and it is not password protected, it is available to whoever is on the SIPRNet.

Senator BROWN. All right. So let me just take what you are saying here—and that was not the case with this young soldier. We are not just talking about that stuff where you just get online and take that stuff. We are talking about that the young person who had the ability to not only get that but all the classified documentation as well. Correct?

Mr. FERGUSON. He was able to get the classified information that was not password protected. That is correct.

Senator BROWN. Right. And is it true that there are hundreds of thousands of people that have access to that information still?

Mr. FERGUSON. That is true.

Senator BROWN. Once again, I am not a brain surgeon, but I am an officer in the U.S. military, and I have difficulty getting that stuff. Why haven't we locked down and basically weeded through the people that have access, to make sure they are all our friends? Where is the command and control in these types of things?

Mr. FERGUSON. The command and control, since the SIPRNet is really a family of networks, the site owners decide, just like on the Internet, who gets access to their particular site.

Senator BROWN. Right. That is for the open stuff, but I am not talking about that.

Mr. FERGUSON. No. That is for secured information as well.

Senator BROWN. All right.

Mr. FERGUSON. So in the case, of course, of the State Department information, that has now been removed from SIPRNet, so that is not available for everybody to take a look at.

Senator BROWN. I was kind of surprised they were even on there.

Mr. FERGUSON. Well, that was a request of the Department of Defense and the DNI to put that information on or to make it more accessible to people in the intelligence community.

Senator BROWN. Is the reason why because—listen, I understand the moving nature of the battlefield. I believe that a lot of the command and control went away because of the changing nature of the battlefield. They needed the information very quickly. Is that a fair assessment?

Mr. FERGUSON. That is a fair assessment.

Senator BROWN. So knowing that, what checks and balances have been put in place, notwithstanding that fact, what are we doing?

Mr. FERGUSON. What they have done—and Ms. Takai can talk about the technology behind this. They have closed down all the ports. They cannot remove the data. But they also are starting to chart and narrow the data access based on mission responsibility, for one. It is not going to be as simple as just going in, turning off stuff, and just doing a big survey of the SIPRNet, although that will probably occur. And then, of course, the moving of the data, which was the big concern, is now a two-man rule. As Ms. Takai pointed out, 12 percent of the systems now have the ability to remove data and shift it to another domain. The other 88 percent are shut down.

Senator BROWN. Well, he used a thumb drive, right?

Mr. FERGUSON. He used a compact disc (CD), actually. Oddly enough, the thumb drives have been shut off for some time.

Senator BROWN. That is what I thought. So it was a CD, right?

Mr. FERGUSON. It was CDs, that is right. He was downloading the CDs. So we have a two-man rule.

Another key piece of this is—I do not know the word to use—a failure on the part to monitor and follow security regulations. It is as simple as that.

Senator BROWN. Listen, I agree with you. I know there is a protocol in place. I am still flabbergasted. I mean, here we are, we have one of the biggest leaks in my lifetime or my memory, at least, in the military, and we have a private who is in trouble. I am a little curious. There seems to have been a breakdown completely on that chain of command.

Mr. FERGUSON. It did not work as well as we had hoped.

Senator BROWN. And that being said, it has not worked as well as you had hoped, is there anything like a red team or an unannounced inspection? Or have you changed the protocol?

Mr. FERGUSON. Actually there have been investigations looking at the entire process for the entire theater. And a lot of the changes have occurred in terms of the two-man rule, shutting down of the ports, and other security training and so forth has all occurred in the last 3 or 4 months. So, yes, they have taken some pretty significant actions already.

If I may, I would like to pass it to Ms. Takai because she can speak to some of the technology that is in place.

Senator BROWN. And with that, I will take that testimony in a second. But that being said, I know all the agencies are actually awash with new guidelines and directives. Is there a coordinated effort of some kind being made so that policy and oversight are staying consistent, that agencies are not left to guess who to listen to? Is there someone in charge that basically is dictating what we are doing, why we are doing it, how we are doing it, and then following up to say, yes, we are, in fact, doing it? Is there anything like that going on?

Mr. FERGUSON. Yes, I will give you a good example. Their policies for security and use of material was spread across a number of policy documents, so if you were sitting in a field or you are in the United States and you wanted to find where that policy was, you had to go search for it. In hindsight, that was not a good way of approaching it. It worked that way for years, decades.

One of the things we have done is we have updated those policies, and we combined and consolidated them into a single product. So there is only one place—it is a one-stop shop to go get that. That came out of the Under Secretary of Defense for Intelligence's office. So he sets the guidelines for that information protection assurance and security parts.

In terms of setting rules for information sharing itself, that is being done as a community-wide activity, not just with the Department of Defense but with the DNI—this is an approach with all the other agencies. So there is one initiative right now underway, and, of course, each department is also looking at it individually.

Mr. PAUL. Can I amplify that?

Senator BROWN. Yes, please, and then I just have one final question, but sure, yes, absolutely.

Mr. PAUL. So there is an ongoing White House-led process right now looking at the WikiLeaks incident and potential structural reforms. That has three main tracks that are going on, and my panelists and I and others are involved in that process.

The first part of it is looking at how to better balance things like identity management and tagging of information more consistently so you can do better kinds of access controls like what were talked about in the opening statements.

The second is looking at the insider threat passbacks and some of the technical considerations that we have talked about.

And the third is looking at how we strengthen governance across the spectrum—so the hope is that in the coming weeks and months we can come back and talk about the results of that process.

Ms. TAKAI. Before I speak to the technology, just to follow on to the governance issue, there is participation by all of the organizations in a White House working group that reports to the deputy's

committee around the various activities to make sure that we are well coordinated and that we are working together.

Inside the Department of Defense, this is an item that is high on the Secretary's list, and we provide ongoing reports to him from the standpoint of the technology mitigation efforts both to him and the Chairman of the Joint Chiefs of Staff regarding our progress. So there is significant oversight. There is significant guidance in terms of making sure that we are taking care of this and we are following on to the commitments that we have made both from a technology perspective and working with Mr. Ferguson's area in terms of making sure that the policies are updated. So I wanted to make sure that I added that in response to the question.

Moving on to the technology, I think we have talked about the Host Based Security System and the progress that we have made thus far in terms of having that installed and making sure that we can detect anomalous behavior in terms of individuals who might get on to the network and download information, and we are doing that in three ways. One is from a device perspective. The Host Based Security System detects if, in fact, a computer does have a device where information can be downloaded so that we can validate that and ensure that it is a part of the 12 percent of those computers that we believe need that information in the field.

The second thing that we are doing is to look at what we call an audit extraction module to follow on to Senator Collins' question around how do we have the information and the analytics to see anomalous behavior and we can catch it at the time that it occurs. We are currently in testing. That software is integrated with HBSS, and we will then be moving ahead to roll that out across DOD.

The third thing that we are moving forward on, as you mentioned, Senator Collins, is around really a role-based process. We are going to be implementing a public key infrastructure (PKI) identification similar to our current Common Access Cards (CACs) that we have on our non-classified network to all of the DOD users, and what that will do is give us an opportunity over time to refine what information individuals have access to. So sheer access to SIPRNet, for instance, in this case, we will be able to, by looking at each individual database, take it down to what information that individual needed as opposed to having the network completely open.

Senator BROWN. I appreciate that, and just in closing, it was not only dangerous, it is embarrassing what happened. You know, it is embarrassing for our country some of the things that were actually out there. And so there are a lot of lessons there, but I appreciate the opportunity.

Thank you for having this hearing and participating and allowing me to participate in it.

Senator COLLINS. Thank you.

Chairman LIEBERMAN [presiding]. Senator Collins, thanks very much for assuming the Chair. I apologize to the witnesses.

I appreciate the testimony. Let me ask a few questions, if I might. In a speech that DNI General Clapper gave last fall, he predicted that WikiLeaks was going to have a "very chilling effect on the need to share." After WikiLeaks began to release State Depart-

ment cables in late November, news headlines forecasted a clampdown on information sharing, and this is what we have been dealing with and you deal with in your testimony as submitted.

I wanted to ask you if there are specific areas—and I guess I would start with Ms. Stone and then any others. Are there specific areas where you think the WikiLeaks case has had a direct impact on information sharing other than the examples cited in the prepared testimony by Mr. Kennedy of the State Department removing its diplomatic cables from SIPRNet?

Ms. STONE. Thank you for that question, sir. My reaction is that the most direct impact has been in the area of culture and those people who are concerned about sharing information, rightly so, and our ability to protect it. And, therefore, our reaction to WikiLeaks must be to increase protection as well as sharing. As we increase the protection, we also increase the trust and confidence that people have that when they share their information appropriately, it will be protected; we will know where the information is; we will be able to pull that information if it is inappropriately accessed; and we will be able to follow up with appropriate repercussions if and when it is misused.

So I think the most direct impact I have seen is not in a specific tangible action, but more so that it has resulted in a very clear need for us to increase the protections, to increase trust and confidence to share more broadly; because—while Director Clapper was very concerned—as we all were, that this would have a chilling effect, we have all worked very hard, both within the ODNI, within the intelligence community, and across the government, to ensure that it does not have a chilling effect; but that, in fact, as Mr. Ferguson said, as we increase sharing, we also increase protection to develop that trust and confidence.

Chairman LIEBERMAN. That is good. Mr. Kennedy.

Mr. KENNEDY. If I could, Mr. Chairman. I think there have been two kinds of chilling effects. One, I think there has been a chilling effect on the part of some foreign governments being willing to share information with us, and that is obviously of great concern to the State Department. We build our diplomatic reporting analysis on the basis of trust; that when individuals tell us things in confidence, we will share them in confidence within the U.S. Government, that it will not go broader than that. So that has been one chilling effect.

I think the State Department, though, has avoided the chilling effect that you were directly addressing. For example, if I might, during the period of time, we have posted, as you all mentioned, some 250,000 cables to this database posted to the DOD SIPRNet. During that same period of time, we disseminated 2.4 million cables, 10 times as many, through other systems to the 65 other U.S. Government agencies. And so, therefore, while we stopped disseminating on SIPRNet for the reasons that my DOD colleagues have outlined, we have continued to disseminate to the intelligence community system, the Joint Worldwide Intelligence Communications System (JWICS), and we have continued to disseminate the same volume of material to the same other agencies based upon their need for that information. We do not hold anything back. This unfortunate event has not caused us to hold anything back. We con-

tinue to share at the same rate as we were sharing before because we know that our information is essentially the gold standard.

There are more reporting and analysis officers and sources and information from 265 State Department diplomatic and consular posts around the world than any other agency, so it is our intent to uphold our piece of national security and obviously to be responsive to the very forceful and correct legislation that you saw past, which is to share. We are continuing to share using two other means.

Chairman LIEBERMAN. Do any of the other three witnesses want to comment, either in terms of specific areas of the effect of WikiLeaks on information sharing or perhaps some more indirect impact with people becoming more hesitant to work across agency boundaries or even marking intelligence products more restrictively? Mr. Paul.

Mr. PAUL. Yes, in my role I have the opportunity to work closely with our State, local, and tribal partners, and I just want to report that the concerns about a chilling effect, they share that. They share the concern, and we remain vigilant and work with them to try to identify any challenges of that sort. But so far with our partners, primarily FBI and DHS, there is a lot of good sharing. Our different sharing initiatives continue to move forward, things like the Nationwide Suspicious Activity Reporting Initiative, the Nationwide Network of Fusion Centers, and different initiatives of those ilk.

Chairman LIEBERMAN. Good. Thanks for your answers to that.

Incidentally, one of the things I have found that I am sure other Members of Congress have found in foreign travel that we have done since the WikiLeaks leaks is that, somewhat in jest but not really, often leaders of foreign countries that we are meeting with will say, "I hope this is not going to appear on WikiLeaks." So they are hoping that there is a certain confidence and trust in the exchange of information. And, of course, we say, "Oh, no." And then the person from the embassy usually says, "No, we have taken care of that problem." But it did affect the trust of allies around the world.

One of the things that Congress called for in the Intelligence Reform and Terrorism Prevention Act was the use of technologies that would allow "role-based access" to information in government systems—in other words, that people would have access to information necessary for their work, but would not have overly broad access to information that they did not need.

One of the key lessons, obviously, from WikiLeaks is that we have not yet made enough progress toward that goal as we need to, and if such capabilities had been in place on SIPRNet, I presume Private Manning would never have had access to that much information, if any at all.

Ms. Takai, maybe we will start with you. What are the key challenges associated with implementing role-based access as I have defined it across our classified and sensitive information systems?

Ms. TAKAI. Thank you, Mr. Chairman. I would like to start first by just giving you an update on where we stand at DOD in terms of rolling out a PKI-based CAC card for SIPRNet.

Chairman LIEBERMAN. Good.

Ms. TAKAI. We are in the process and, in fact, they are in production, if you will, through our trusted foundry on those cards. We are anticipating the completion of the rollout by the end of 2012 so that all the individuals who today need SIPRNet and use SIPRNet will have PKI identification.

Chairman LIEBERMAN. Have you defined those terms while I was away? Or would you want to do so now, PKI and the CAC card, for the record?

Ms. TAKAI. Effectively the common access card is a card that you actually utilize with your computer that actually identifies you when you log on to the computer. So it is a much more sophisticated password, if you will. It gives you a user name and password, but it more clearly identifies you, and then from that more clearly can identify the role that you play in the organization and then through that the information to which you should have access.

Chairman LIEBERMAN. So that would all limit access based on what the position of the card holder was and the presumed needs to know of the card holder.

Ms. TAKAI. That is correct, sir. But to the second part of your question in terms of our rollout plan and the steps that we need to go through, the cards are actually rolled out to each individual who has a computer, so our deployment plan is to actually get the physical cards and the physical readers installed on all of the computers for those individuals that require access to SIPRNet.

The second thing is that through the trusted foundry we have a manufacturing process for those cards, and they have a capacity for a certain number of cards, so that also is a factor.

So, again, in order for us to really complete 100 percent, we have to take into account those two factors, and also the fact that many of the computers where this is needed are, as you could well imagine, in many locations around the globe. And that is not only, of course, certainly on the ground, but on ships and so on. So it will take us a while, by the end of 2012, to have that deployment complete.

But I think it is important to note, in addition to just the physical deployment of the cards and on the various computers, that it will then take us additional time to make sure that we get the roles associated with the information connected. So the cards give us the capability to do that, and then we will continue the deployment to link the information to that.

Chairman LIEBERMAN. That is encouraging. Thanks. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman. Just a couple more questions.

Mr. Ferguson, when I think about the WikiLeaks incident, I think not only of the failures of technology but also a failure to focus on certain red flag behavior that was exhibited by the suspect. And it reminds me very much of what our investigation found when we looked into Major Hasan's behavior prior to the massacre at Fort Hood.

If the media reports are correct, Private Manning exhibited problems such as mental health issues, an assault on colleagues, and the fact that supervisors had recommended that he not be sent to the front lines.

These are all pretty big red flags, and I am wondering why they did not lead to a restriction in his access to classified information. I do not know whether you are the right person for me to ask that question to, but my point is there is more than just technology at stake here. If we have a high-ranking official and we use the user role approach but that individual becomes unstable or embraces Islamist radicalism or there is some other reason that would cause the individual to pose an insider threat, do we have the systems in place to catch that individual?

Mr. FERGUSON. Senator, I probably cannot really speak to the specifics of Private Manning. It is an ongoing investigation. However, your point, though, about a process to identify behaviors that we should be concerned about, we have taken a look at that, and the training that we had in place—whether it was Hasan or this case—was not sufficient to give his supervisors the pieces of data they would need to put together and say this person is a problem, or in some cases to take action when they did suspect something was wrong.

So what we have done in the Department is begin to shape with new policy and direction how to better train supervisors in how to best identify behaviors that would be of concern. That is one piece, but they also have to be willing to take action, and that is part of the other problem. It is not that somebody might say that this behavior is irregular. It is also in some cases a fear to take action, or it may reflect on them as a failure or it may reflect on them in some other way. And so there are two hurdles here. It is teaching people how to identify the characteristics, but it is also teaching people that the right thing to do is to take action.

Senator COLLINS. I am concerned because we have seen two recent cases where tremendous damage was done, despite the fact that there was ample evidence, it appears—I am less familiar with the case we are discussing today—that something was dramatically wrong. That is an issue that I am eager to pursue, and I think your point about training is a very good one.

Mr. Paul, just for my last question, you mentioned in your testimony that there is a fragmented approach to computer security across the Federal Government, and I think I can speak for the Chairman when I say that we could not agree with you more, and that is one reason we have introduced our cybersecurity bill which will apply to the civilian agencies and also try to work with the private sector to develop best practices. But our bill does not deal with the intelligence community or the military computer systems.

You also in your testimony pointed out that you are not an operational office at DNI and that you are heading a task force on this issue. What are you telling us? Are you telling us that the DNI needs more authority to prevent this fragmented approach where one intelligence agency may have a totally different approach to security, classification, and access than the Department of Defense?

Mr. PAUL. So when I was using the description of "fragmentation," what I was referring to was that agencies put in place specific agency-based solutions. Those solutions serve for specific needs. But then when you look at more broad information sharing and protection with other agencies, the solutions tend to not work as well. An example of this is, as we look at things like identity

management frameworks—some of my panelists have talked about identity management. That is foundational to being able to do information sharing and information protection. We have several different identity management frameworks across the scope of the Federal Government, our State and local partners, and so forth. Those frameworks are mostly aligned, but we need to make sure that as they get implemented, they are implemented in a way that is consistent across all the different partners. If that does not happen, then you run into challenges when information moves across organizational boundaries.

The second part of your question was about my role in co-chairing the Information Sharing and Access Interagency Policy Committee. A key thing that we are trying to do in that group is to harmonize policy frameworks across the different agencies to make sure that on one hand, we have the consistent framework, but on the other hand, we are not slowing down operational considerations in those agencies so that the variations that occur are truly because of mission requirements and not because we are not effectively working together.

Senator COLLINS. Ms. Stone.

Ms. STONE. Thank you. If I could just add to that, across the intelligence community we are working very hard to have comprehensive guidelines and processes that are consistent and interoperable. We are working on leveraging public key infrastructure and attribute-based access control to have a more comprehensive identity and access management. We are standardizing data protection models to have several levels of security, and we are working on an enterprise audit framework.

So within the intelligence community, while we may have different systems, we are working very hard from the Office of the Director of National Intelligence to more standardize and ensure consistency across those networks. The way we then plug in with the rest of the government—and, indeed, we must be interoperable with the rest of the government, of course—is through this interagency group that we are working on together with everyone at the table and others to ensure that we can, in fact, be coordinating and consistent with the other offices. And we are still working through exactly what that looks like, but that is certainly a concern that we are all very well aware of.

Senator COLLINS. Thank you. Just two final concluding comments. I would note that the Government Accountability Office (GAO) continues to list information sharing, particularly with regard to terrorism-related information, as a high-risk activity, and it is on the high-risk list again this year.

And, finally, as we look at the user role approach, which I brought up in my opening statement and which we have commented on today, we do have to be careful that does not translate back to the bad old days where no one shared anything and where we had stovepipes because we are defining who has access so narrowly that we deny access to analysts who really need that information.

So it is a very difficult task that you are all embarking on, but in this day and age, that an individual could be able, undetected for so long, to download and illegally distribute hundreds of thou-

sands of important cables, reports, and documents is just inconceivable to me. So, clearly, we have a long way to go to strike the right balance.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins, very much. Thanks again for taking the chair while I had to leave.

Just a few more questions, and I want to follow up first with one to you, Mr. Paul, following up on the question I asked Ms. Takai before about role-based access. In your testimony, you note the fact that there are at least five distinct identity credential and access management frameworks in use by Federal agencies, and, of course, that makes me wonder whether that limits the ability to implementation the kind of role-based access capabilities that the IRTPA required in systems in a cost-effective way. I wonder if you could talk about what you are doing, hopefully in cooperation, perhaps, with the other witnesses here today, to harmonize those different access frameworks.

Mr. PAUL. Sure. Thank you for the question. There are these five different frameworks, but they are really not that different. They are different enough, though, that it requires the attention of my office and other bodies—the Federal Chief Information Officer Council, for example, and my colleagues here—to make sure that as the frameworks get implemented in the different agencies and with our State, local, and tribal partners, that we do not allow for variations or that variations are controlled and reflect mission requirements and the like. So a focus of my office is to work with the interagency, bringing together groups to make sure that as these frameworks get implemented, they are implemented in a consistent way.

Building on top of that, it is critical, as we look at role- and attribute-based access controls that you both have highlighted, that the framework for doing those, how we define roles, how we, to use a colloquialism, tag data, how we tag people, and that tagging occurs in different places. A person may be tagged in one agency, data may be tagged in another, and we want to be able to have that data move in an appropriate way with policy enforcement. That means there needs to be a consistent framework for how that happens, and coordination, and this goes to some of what you have heard from me and others about the importance of governance of the standards and architecture approach. So those are contributions that are catalyzed through the efforts of my office in close cooperation with my mission partners.

Chairman LIEBERMAN. Good. I urge you on in that.

Mr. Ferguson, I mentioned in my opening statement the great successes that we have had in the past few years in Iraq and Afghanistan in disrupting terrorist networks in those countries with our military and intelligence agencies working very closely together and doing so in a remarkably rapid way, sometimes exploiting information from one raid or one source and using it within an hour elsewhere, or quicker.

As you make changes to improve the security of classified networks at DOD and in the intelligence community, are you taking steps to ensure that those efforts will not diminish or slow down

our ability to carry out the kinds of operations I have just described?

Mr. FERGUSON. Yes, sir, absolutely. Even though the process was to allow personnel working in a secured facility to access the SIPRNet and pull down data and copy it through open media.

Chairman LIEBERMAN. Right.

Mr. FERGUSON. For example, so we could have more agility and flexibility. We have gone back and taken a look at how that process worked, and we have found that by creating just a kiosk process and a two-man rule, we can still move at the same speed and have the same agility without giving everybody the same availability to the information and being able to pull the data down and copy it. So it is very much in mind to make sure that we do not hinder our ability to carry out the operations.

Chairman LIEBERMAN. Good. Do you want to add anything, Ms. Takai?

Ms. TAKAI. Yes, I would. I think one of the things that is very important is that we continue to see the dramatic need for information and information sharing by the warfighter and so, if anything, the demand for that information continues to grow. And so as we are looking at the technology, just to relate back to what Mr. Paul said, part of our efforts are to ensure within DOD we are eliminating our fragmented environment, which has grown up over time, through our legacy base of the way that our networks and our databases have grown up. And so I wanted to make sure that I added that there was a relationship between the work that Mr. Paul is doing and the work that we are doing internal to DOD, and I am sure my partners here are all undergoing the same thing. I think that is really what Ms. Stone was talking about. And those things in combination with being able to apply cybersecurity enhancements are really going to give us an opportunity to get that information out there as quickly as today and in some cases even faster than today, but to do it in a secure way.

Chairman LIEBERMAN. That is excellent. Let me ask a final question. Based on the testimony you have provided, really in what you are doing to respond to the challenges that were illuminated by the WikiLeaks case, but also to protect the information-sharing environment, one, have you seen any areas where you think you would benefit from statutory changes? And, two—and this is a question that I ask in a limited way in this fiscal environment—are there any funds we should be targeting to particular uses that we are not now doing to assist you in responding to this crisis? Maybe we will start with Mr. Kennedy and go down the table, if anybody has anything to say.

Mr. KENNEDY. Thank you very much, Mr. Chairman. I cannot think of any additional legislative authority. I think you have done two things. You have given us the intent, and then you have given us the command. And I think we know from what you have said and what we know internally which way we should go.

On the funding, I can always say that an institution as small as the State Department can always use additional funding given the range of demands upon us. But I believe that we have a role-based access system in place that we use to distribute material within the State Department. If you are on the French desk, you get one set

of materials. If you are on the Japan desk, you get another. As I mentioned earlier, we will continue to push State Department reporting to the other agencies, but it does, I will admit, put a burden on them to then take our material which we have provided to Secretary of Defense, so to speak, to DOD, and then to distribute that to their people according to the roles that only they are capable of defining, because I think it would be wrong for me to say which individuals within an entity as large as the Defense Department or as large as the DNI or the intelligence community which analyst needs what. So we send it to them, and I think they may be the ones who have to answer that second question about how they are going to distribute it efficiently and effectively as both you and Senator Collins have talked about.

Chairman LIEBERMAN. Thanks. Ms. Takai, any legislative recommendations or budget targeting?

Ms. TAKAI. In terms of the legislative question, I agree with Mr. Kennedy. At this time we do not see any additional legislation that we need. We are going through a review to answer exactly that same question for the Secretary in terms of is there any need for any change, not only additional funding but a change in the cadence of the funding. And so once we have that pulled together, we would be happy to share it with you.

Chairman LIEBERMAN. I appreciate it. Mr. Ferguson.

Mr. FERGUSON. I would have to agree on the legislative side, and certainly as Ms. Takai has pointed out, as we go through this process of putting in these capabilities, what kind of funding needs I guess we have to identify what those real costs are and come back.

Chairman LIEBERMAN. Ms. Stone.

Ms. STONE. Similarly, on the legislative question, I think we have what we need for now, although I would reserve the right to come back if we discover we need something else.

And on the funding piece, again, we do have an interagency process ongoing looking at exactly what we might do with different options, so we would have to see where that comes out. But I do believe there is at least something in the fiscal year 2012 proposal submitted by the President to work on some of these issues.

Chairman LIEBERMAN. Good. Mr. Paul.

Mr. PAUL. Just to echo Ambassador Kennedy, the laws and the statutes that this Committee has championed provide an adequate basis, a fine basis. I know in the context of the information-sharing environment that it is my responsibility, there is enough authority. It is an issue for me now of execution and leadership.

Chairman LIEBERMAN. Good. Thank you all. Senator Collins.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Well, thanks very much, again, for your prepared testimony and the oral testimony, and I emerge encouraged that you are certainly dealing with the specific series of vulnerabilities that the WikiLeaks/Manning case revealed, and I presume in the nature of the modern world with technology, innovation, and exploitation what it is, you will also be thinking about the next way in which somebody might try to take advantage of our information-sharing environment. But I think that we have raised our guard in a sensible way and also continue to share infor-

mation, which we need to do, is what I take away from this hearing, and I appreciate that very much.

The record will remain open for 15 days for any additional questions or statements. With that, the hearing is adjourned.

[Whereupon, at 4:36 p.m., the Committee was adjourned.]

APPENDIX

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph Lieberman
"Information Sharing in the Era of Wikileaks: Balancing Security and Collaboration
Homeland Security and Governmental Affairs Committee
March 10, 2011
As Prepared for Delivery

The hearing will come to order. Good afternoon and thanks for your patience. In just six months and a day we will mark the 10th anniversary of the attacks of 9/11 and we will honor the memory of the nearly three thousand people who were murdered that day in America.

Our mourning over their deaths has always been compounded by the knowledge that those attacks might have been prevented, certainly that was the implication of the 9/11Commission report, had our intelligence and law enforcement agencies shared the disparate facts they had gathered, enabling us to connect the dots.

To prevent this from happening again, Congress passed several laws intended to strengthen information sharing among critical federal agencies. Those acts included the Homeland Security Act, the Intelligence Reform and Terrorism Prevention Act and the Patriot Act.

Since then, the executive branch, I think, has made significant improvements in its information sharing systems and there is no question that far more information is now available to partners in other agencies who have a legitimate need for it.

All this intelligence is further brought together at key nodes, such as the National Counterterrorism Center, where it can be examined by intelligence specialists from a variety of agencies working together under one roof.

And, as a result, we have seen a number of successes in recent domestic and military counter-terrorism operations that I think were thanks to this information sharing – and I'm going to cite some examples in a moment.

But this Committee's recent report on the Fort Hood attack shows that information sharing within and across agencies is nonetheless still not all it should be – and that allowed in that case a "ticking time bomb" namely Maj. Nidal Hasan, now accused of killing 13 and wounding 32 others at Fort Hood– to radicalize right under the noses of the Department of Defense and the FBI.

So we need to continue improving our information sharing strategies. Now, I fear, the Wikileaks case has become a rallying cry for an overreaction for those who would take us back to the days before 9/11 when information was considered the property of the agency that developed it and was not to be shared.

The bulk of the information illegally taken and given to Wikileaks would not have been available had that information not been on a shared system, the critics of information sharing argue.

But to me this is putting an ax to a problem that requires a scalpel and misunderstands that happened in the Wikileaks case and misstates the solution to the problem. We can and must prevent another Wikileaks without also enabling federal agencies, perhaps compelling federal agencies to reverse course and return to a pre-9/11 culture of hoarding information.

We need to be smarter about how information is shared, and appropriately balance security concerns with the legitimate needs of the users of different types of information. Methods and technologies for doing so already

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000033 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT
66677.001

exist, some of them I gather have been put into place since the Wikileaks case, and we need to make sure that we utilize them as fully as possible across our government.

The bottom line is we must not walk away from the progress that has made us safer and saved lives. I'll give you two quick examples:

U.S. Special Forces and elements of the intelligence community have shared information and worked exceptionally well together in war zones to combat and disrupt terrorist groups such as Al Qaeda in Iraq and the Taliban in Afghanistan. And that would not happen without information sharing.

Here at home, we have used information sharing to enhance the role of state, local, tribal and private sector entities in our fight against terrorists.

And those efforts have paid off – most recently in the case of a chemical supply company in North Carolina that alerted the FBI to suspicious purchases by a Saudi Arabian student in Texas who turned out to be building Improvised Explosive Devices.

So we need to fix what is broken without going backwards. Today I look forward to hearing from each of our witnesses about what they are planning to do to improve the security of classified networks and information, while still ensuring that information is shared effectively in the interest of our nation's security.

I also want to hear how Congress can work with you on these efforts with either legislation or through more targeted funding.

Efficiently sharing, while effectively securing, information is critical to our nation's security and our national values. We can and must have both.

-30-

Statement of Ranking Member
Susan M. Collins

"Information Sharing in the Era of Wikileaks: Balancing Security and Collaboration"

March 10, 2011

★ ★ ★

Effective information sharing among federal law enforcement and civilian and military intelligence agencies is critical. The 9/11 Commission found that the failure to share information across the government crippled efforts to detect and prevent the attacks on September 11th, 2001. Improving this communication was a critical part of the Intelligence Reform and Terrorism Prevention Act that Senator Lieberman and I authored in 2004.

The WikiLeaks breach should not prompt a knee-jerk retreat on the sharing of information and its use by those analysts who need it to do their jobs. We must not let the astonishing lack of management and technical controls that allowed a Private in the Army allegedly to steal some 260,000 classified State Department cables and 90,000 intelligence reports to send us back to the days before September 11th.

Unfortunately, we continue to see agency cultures that resist sharing information and coordination with their law enforcement and intelligence counterparts. Almost 10 years after 9/11, we still witness mistakes and intelligence oversights reminiscent of criticisms predating our reforms of the intelligence community. Among those cases where dots were not connected and information was not shared are: Umar Farouk Abdulmutallab, the so-called Christmas Day bomber, and Nidal Hasan, the Fort Hood shooter.

At the same time, there have been several cases that underscorce the incredible value of information sharing. An example is the case of Najibullah Zazi, whose plans to bomb the New York City subway system were thwarted.

As such successes remind us, we must not allow the WikiLeaks damage to be magnified twofold. Already, the content of the cables may have compromised our national security. There have been news reports describing the disclosure of these communications as having a chilling effect on our relationships with friends and allies. More important, they likely have put the lives of some of our citizens, soldiers, and partners at risk.

Longer lasting damage could occur if we allow a culture to re-emerge in which each intelligence entity views itself as a separate enterprise within the U.S. counterterrorism structure, with each attempting to protect what it

66677.003

considers its own intellectual property by not sharing with other counterterrorism agencies.

Such a step backward would run counter to the policy goals embodied in the Intelligence Reform Act, articulated by law enforcement and intelligence community leadership, and underscored in multiple hearings before this Committee; that is, to effectively detect and interdict terrorists, the "need to share" must replace the "need to know."

I also would like to hear about the possible technological solutions to this problem. For example, my credit card company can detect out-of-the-ordinary charges on my account almost instantaneously. Yet, the military and intelligence community were apparently unable to detect more than a quarter million document downloads in less than nine months. Surely, the government can make better use of the technology currently employed by the financial services industry.

It is also notable that the intelligence community was already required to install some audit capabilities in its systems by the 2007 homeland security law, which could have included alerts to supervisors of suspicious download activity. Had this kind of security measure been in place, security officers might have detected these massive downloads before they were passed on to Wikileaks.

Technology and innovation ultimately should help protect information from unauthorized disclosure, while facilitating appropriate sharing of vital information.

I also would like to explore the implementation of "role-based" access to secure classified information. Instead of making all information available to everyone who has access to classified systems, under this model information is made available in a targeted manner based on individuals' positions and the topics for which they are responsible. Access to information not directly relevant to an individual's position or responsibilities would require a supervisor's approval.

We must craft security solutions for the 21st Century and beyond. We are in a world of Tweets and instantly viral videos on YouTube. We must strike the proper balance that protects classified and sensitive information with ensuring the sharing of vital data. We can use the most cutting-edge technology to protect the traditional tools of statecraft and intelligence - relationships and information.

STATEMENT OF AMBASSADOR PATRICK KENNEDY
UNDER SECRETARY FOR MANAGEMENT
U.S. DEPARTMENT OF STATE
Before the Senate Committee on
Homeland Security and Governmental Affairs
"Information Sharing in the Era of WikiLeaks:
Balancing Security and Collaboration"
March 10, 2011

Chairman Lieberman, Ranking Member Collins, Members of the Committee, good afternoon and thank you for this opportunity to appear before you today to address the status of information sharing in light of the WikiLeaks disclosures, and in particular to discuss efforts within the executive branch both to improve the security of its systems, and to ensure that information is shared effectively and in a manner that continues to advance national security objectives. The Department of State and our interagency partners here today have long been closely engaged in achieving the dual objectives of appropriate information-sharing and protection, and in light of the WikiLeaks compromises, we are working together with renewed attention on achieving these dual objectives.

As you may be aware, I bring a rather unique perspective to the challenges of sharing and protecting information. I have served most of my career at the State Department -- overseas, at the United States Mission to the United Nations and here in Washington, and I was also honored to serve as the first Deputy Director of

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000037 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.005

National Intelligence for Management at the creation of the Office of the Director of National Intelligence (ODNI). Given this experience, I especially appreciate the commitment of this Committee to work with us in addressing the challenges of information security and sharing. Despite events of the past eight months, I want to assure Members of this Committee at the outset that we at the State Department maintain our commitment to fully share our diplomatic reporting on which our interagency partners rely. Our collective challenge is to do so in a manner that provides safeguards and protections that are reasonable, pragmatic, and responsible, not to stop sharing.

The focus of my testimony this afternoon is threefold: first, to explain briefly the Department's unique role within the executive branch as a source of diplomatic reporting that is essential to a variety of different agencies; second, to provide an overview of the State Department's mitigation efforts; and finally, to highlight the challenges as we move forward to share and protect our classified information.

Role of Diplomatic Reporting

The State Department has historically accomplished basic communication between Washington and overseas posts through the use of diplomatic telegrams or cables. These communications serve as the vehicle for our internal deliberations

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000038 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.006

relating to all aspects of our foreign relations and include candid assessments of conditions overseas and of diplomatic instructions that are vital to national-level decision-making. This formal channel between Washington and our overseas posts provides the Department and other U.S. Government agencies crucial information about the context in which we collectively advance our national interests on a variety of issues. For example, these communications may contain information about promoting American export opportunities, protecting American citizens overseas, and supporting military operations. We consider this reporting from posts around the world to be one of our most valuable contributions to every facet of national security, and we share this diplomatic reporting through automatic dissemination to over 65 agencies based on profiled requirements these agencies provide to the Department. Recent events have not changed our commitment to sharing this vital information.

WikiLeaks Disclosures and State Department Mitigation Actions

July 2010

When DoD material was leaked in July 2010, we worked with DoD to identify any alleged State Department material that was in WikiLeaks' possession. We immediately asked Chiefs of Mission at affected posts to review any purported State material in the release and provide an assessment, as well as a summary of

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000039 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.007

the overall effect the WikiLeaks release could have on relations with the host country.

Following the completion of the review in August, when it was believed that purported State cables might be released, the State Department instructed all Chiefs of Missions to familiarize themselves with the content in the Net Centric Diplomacy (NCD) database should a release actually occur.

November 2010

When the press and WikiLeaks announced that they were going to release purported State cables starting on November 28, 2010, the State Department took the following immediate actions: 1) Established a 24/7 WikiLeaks Working Group composed of senior officials from throughout the Department, notably our regional bureaus; 2) Created a group to review potential risks to individuals; and 3) Suspended SIPRNet access to NCD (SIPRNet is a DOD network).

The Department also created a Mitigation Team to address the policy, legal, security, counterintelligence, and information assurance issues presented by the release of these documents. During this period, the Department kept Congress apprised of both the international fallout caused by the WikiLeaks' disclosure and the steps undertaken to mitigate them. The Department convened two separate briefings for members of both the House of Representatives and the Senate within

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000040 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.008

days (December 2, 2010) of the first disclosure by WikiLeaks and appeared twice before the House Permanent Select Committee on Intelligence (December 7 and 9, 2010).

Ongoing Mitigation Efforts

State continues its thorough review of policies and procedures related to information security to ensure that they fully meet the current challenges. Efforts are being coordinated throughout the Department, as well as with the interagency, to ensure that we share classified information in an effective and secure manner with those who need it in their work to advance our national security.

- While the Department already had strong safeguards in place, we have further enhanced and updated our computer security policies that prohibit the downloading of classified information to removable media (e.g., thumb drives, CDs/DVDs) on the Department's classified network.
- The Department continues to deploy an automated tool that audits and monitors the Department's classified network to detect anomalies that would not otherwise be apparent. This capability is backed up by professional staff who promptly analyze detected anomalies to ensure that they do not represent threats to the system.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000041 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.009

- The NCD database of diplomatic reporting and the State Department's classified web sites, although now inaccessible through SIPRNet, remains available via the more limited distribution Joint Worldwide Intelligence Communications System (JWICS). Throughout, the State Department has continued to share its diplomatic reporting among federal agencies through its traditional system of cable dissemination.
- To heighten awareness of what is and is not permitted when working on the Department's classified network and on classified systems, user awareness reminders are now available for Department employees on its classified network, in addition to the standard in-person briefings about handling classified material and a soon-to-be-released computer-based course on identifying and marking classified and sensitive information.

In addition, the Department is exploring solutions to improve how we share and protect information with those who are not direct recipients of our telegrams. One such solution would involve the creation of a website with a searchable database that would allow appropriately cleared personnel to use key word searches to discover relevant State cables; the search would reveal cable metadata, such as the subject line, but would not provide the full text of the cables in a potentially vulnerable database. This would ensure that cleared personnel are aware of cables they have an operational or strategic need to see. Cleared

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000042 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.010

personnel from other agencies would then be able to seek cables necessary for their work functions through their own organization's internal distribution system. The responsibility will be on the receiving, not the originating, agency to disseminate information to its internal personnel.

The Department has continued to work with the interagency on information management issues by participating in meetings of the new Interagency Policy Committee (IPC) chaired by the Special Advisor for Information Access and Security policy as well as existing IPCs such as the Information Sharing and Access IPC.

Challenges

The interagency is grappling with the complexities of three main challenges in the aftermath of WikiLeaks.

The first main challenge is ensuring information sharing policies are consistently directing the use of technology to solve problems, not the other way around. The post-9/11 mindset was focused on providing technical solutions to information sharing problems. As a result, technical experts were asked to develop solutions to the barriers inhibiting information sharing. The post-WikiLeaks environment reminds us that technology is a tool to execute solutions but is not in

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000043 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.011

itself the answer. Simply put, we must more consistently sort out what we share before determining how we share it. Connecting systems and networks may provide the means to share information, but we must still manage and share the content in the most appropriate way.

Mr. Chairman, the national security community must do a better job of articulating what information is appropriate to share with the widest appropriate distribution, and what is more appropriately confined to a narrower audience, in order to ensure adequate safeguards. The State Department believes that the way in which we share cables through our traditional means of dissemination and the steps we have taken already since November are leading us firmly in this direction.

The second main challenge involves each agency's rigorous adherence to existing, or improved, information security policies. This includes improved training of cable drafters in the use of labels to indicate appropriate breadth of dissemination based on the sensitivity of a cable's content. The executive order on classified information (E.O. 13526) establishes the basic levels of classification within the Executive Branch. From that foundation, individual agencies may still have their own captions that denote how information should be disseminated because not all cleared personnel need to see every diverse piece of classified information. Agencies that receive information need to understand how to handle

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000044 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.012

that captioned information, so that it is not inappropriately made available to a wide audience, which would undermine the intent of the captions.

The Office of Management and Budget (OMB) directed agencies to create teams to address security, counterintelligence, and information assurance issues. We believe that the State Department's Mitigation Team serves as a model for broad, cross-discipline coordination, or governance, because it brings together various subject matter experts from different fields to address information sharing and security issues in a coordinated manner. Many information sharing and security issues can be resolved at the agency level as long as there are standards in place for agencies to execute. For the most part, standards have been created by existing interagency bodies, but there are some areas where further coordination is needed.

The third main challenge involves the coordination, or governance, of information management in the interagency community. Numerous interagency groups are wrestling with issues related to the technological aspects of information sharing, such as those dealing with data standards, systems, and networks. Others are wrestling with the policy decisions of who should have access to what classified information. New interagency governance structures to coordinate information sharing have been developed, including those focused on sharing with state, local, and tribal governments, as well as with foreign partners. In keeping

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000045 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.013

with the first main challenge, these new structures should maintain or increase their focus on defining the content to be shared and protected as well as on the technology by which it is shared and protected. Each agency must be confident that security processes and procedures are applied in a uniform and consistent manner in other organizations. In addition, it must be understood that material originating in one agency will be treated by other agencies in accordance with mutually understood handling instructions.

The State Department shares information with the intent of providing the right information to the right people at the right time. We will continue to share this reporting appropriately so that we can continue our diplomatic mission as well as our role in the national security community. We recognize the imperative to make diplomatic reporting and analysis available appropriately with the interagency community. We continue to review how our information is disseminated at other agencies.

Conclusion

To recap, the State Department has long been, and remains, committed to both appropriately sharing and protecting information critical to our national security. This commitment requires ongoing efforts to confront multiple, complex challenges associated with information sharing. First, national security agencies must consistently put policies about content ahead of technological solutions.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000046 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.014

Second, each agency must manage the sharing and protecting of information it originates and receives. Third, the interagency as a whole must continue to coordinate better to improve all facets of information sharing.

Thank you for this opportunity to appear here today. I look forward to working with the Committee on the challenges of sharing and protecting diplomatic and other sensitive information, and would be pleased to respond to any questions you may have.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000047 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.015

Joint Statement for the Record

Senate Homeland Security and Government Affairs Committee

Hearing on Information Sharing in the Era of WikiLeaks:
Balancing Security and Collaboration

March 10, 2011

Ms. Teresa Takai
Chief Information Officer and
Acting Assistant Secretary of Defense for Networks and Information Integration

Mr. Thomas Ferguson
Principal Deputy Under Secretary of Defense for Intelligence

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000048 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.016

Chairman Lieberman, Ranking Member Collins and distinguished Members of the Committee, thank-you for the invitation to provide testimony on what the Department of Defense (DoD) is doing to improve the security of its classified networks while ensuring that information is shared effectively.

The 9/11 attacks and their aftermath revealed gaps in intra-governmental information sharing. Departments and agencies have taken significant steps to reduce those obstacles, and the work that has been done to date has resulted in considerable improvement in information sharing and increased cooperation across government operations. However, as we have now seen with the WikiLeaks compromises, these efforts to give diplomatic, military, law enforcement and intelligence specialists quicker and easier access to greater amounts of information have made our sensitive data more vulnerable to compromise. The expanded use of computer networks has also increased the opportunity for even a single authorized user to access, copy, manipulate, download, and intentionally publicize enormous amounts of information from the interconnected databases of multiple agencies. As part of an integrated federal government approach, DoD has taken and continues to take steps to prevent such compromises from happening again.

SIPRNet - Background

Before discussing the particulars of the WikiLeaks incident and the exfiltration of classified documents from the DoD Secret Internet Protocol Router Network (SIPRNet), we would like to first provide a brief overview of the SIPRNet and explain why classified information is widely shared on this network and others like it.

In the mid-1990s, DoD created a network that functions like a classified internet. This network, called SIPRNet, is principally used as a means of posting and sharing essential command and control, mission planning and execution, and intelligence information – particularly among war fighters and command headquarters. Every SIPRNet connection is physically protected and cryptographically isolated, and each authorized user must have a SECRET-level clearance. SIPRNet connects approximately two thousand DoD locations and has between 400,000 and 500,000 DoD users.

One can think of SIPRNet as a classified DoD internet that connects DoD classified local area networks with each other and with classified networks across the government. Each local area network hosts its own organization's classified information services on SIPRNet and selects which elements of its information to make accessible to the larger network. Most information is made available on web pages supported by

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000049 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.017

search engines. A search on a subject will return links to information available on any Department or Agency network connected to SIPRNet that grants the authorized searcher access to that data.

WikiLeaks Disclosures and Immediate DoD Actions

In late July 2010, Wikileaks released thousands of classified DoD documents related to the War in Afghanistan – the first disclosure of several to follow. In late October 2010, Wikileaks released 400,000 classified Iraq logs, and in late November 2010 Wikileaks began an ongoing release of State Department diplomatic cables.

On August 12, 2010, immediately following the first release of documents, the Secretary of Defense commissioned two internal DoD studies. The first study, led by the Under Secretary of Defense for Intelligence (USD(I)), directed a review of DoD information security policy. The second study, led by the Joint Staff, focused on procedures for handling classified information in forward deployed areas. The Secretary also tasked the Director of the Defense Intelligence Agency to stand up an Information Review Task Force to assess, in concert with interagency participants, the substance of the data disclosed.

Results of the two studies revealed a number of findings, including the following:

- Forward deployed units maintained an over-reliance on removable electronic storage media.
- Roles and responsibilities for detecting and dealing with an insider threat must be better defined.
- Processes for reporting security incidents need improvement.
- Limited capability currently exists to detect and monitor anomalous behavior on classified computer networks.

Once the studies were concluded and the results reported to the Secretary, the Department began working to address the findings and improve its overall security posture to mitigate the possibility of another similar type of disclosure. Some of this work was already planned or underway. For other findings, like the issue of removable media, new initiatives had to be immediately implemented.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000050 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.018

DoD Technical Mitigations Efforts

The most expedient remedy for the vulnerability that led to the WikiLeaks disclosure was to prevent the ability to remove large amounts of data from the classified network. This recommendation, forwarded in both the USD(I) and Joint Staff assessments, considered the operational impact of severely limiting users' ability to move data from SIPRNet to other networks (such as coalition networks) or to weapons platforms. The impact was determined to be acceptable if a small number of computers retained the ability to write to removable media for operational reasons and under strict controls.

The preferred method to accomplish this was by means of security software the Department is deploying to all of its workstations – the Host Based Security System (HBSS). HBSS provides very positive technical control over the machines and reports on machine configurations which can be centrally monitored. In this particular case the Device Control Module (DCM) on HBSS is used to disable the use of removable media. For those few machines where writing is allowed HBSS will report, in real time, each write operation. It will also report every attempt of an unauthorized write operation. Where HBSS is not yet fully deployed other means are used to disable write capability, such as removing the software used to write to CDs, removing the drives themselves from the machines, or blocking access to external devices in workstation configuration files.

The Department has completed disabling the write capability on all of its SIPRNet machines except for the few – currently about 12% – that maintain that capability for operational reasons. The great majority of these are disabled using HBSS, so we have positive visibility into their status. We will complete installation of HBSS on SIPRNet in June 2011. The machines that maintain write capability for operational reasons are enabled under strict controls, such as using designated kiosks with two-person controls.

DoD Policy Review

Not all of the actions necessary to ensure information security are focused on technical solutions. The Defense Security Service (DSS) is developing web-enabled information security training that will become part of the mandatory information assurance training conducted annually across the Department. Five separate policies are now combined in an updated version of DoD's Information Security Program policy.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000051 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.019

Some examples of work already underway include last year's stand-up of the first defense security oversight and assessment program. The program reaches out to defense components to understand strategic issues for the enterprise, highlight best practices, and monitor compliance with DoD security policy. In addition, the Joint Staff is establishing an oversight program that will include inspection of forward deployed areas.

To establish better governance over cross-functional responsibilities for insider threats, the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD(HD&ASA)) was appointed the lead across the Department for standing up a formal insider threat program. ASD(HD&ASA) is developing a concept of operations which will ultimately be briefed to the Secretary.

Access Controls

One of the major contributing factors in the WikiLeaks incident was the large amount of data that was accessible with little or no access controls. Broad access to information can be combined with access controls in order to mitigate this vulnerability. While there are many sites on SIPRNet that do have access controls, these are mostly password-based and therefore do not scale well. The administration of thousands of passwords is labor intensive and it is difficult to determine who should (and should not) have access.

DoD has begun to issue a Public Key Infrastructure (PKI)-based identity credential on a hardened smart card. This is very similar to the Common Access Card (CAC) we use on our unclassified network. We will complete issuing 500,000 cards to our SIPRNet users, along with card readers and software, by the end of 2012. This will provide very strong identification of the person accessing the network and requesting data. It will both deter bad behavior and require absolute identification of who is accessing data and managing that access.

In conjunction with this, all DoD organizations will configure their SIPRNet-based systems to use the PKI credentials to strongly authenticate end-users who are accessing information in the system. This provides the link between end users and the specific data they can access – not just network access. This should, based on our experience on the unclassified networks, be straightforward.

DoD's goal is that by 2013, following completion of credential issuance, all SIPRNet users will log into their local computers with their SIPRNet PKI/smart card credential. This will mirror what we already do on the unclassified networks with CACs.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000052 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.020

Our intention is for all SIPRNet web servers to require PKI credentials by mid-2013, again mirroring what's been done on our unclassified network. Beyond that, DoD components will modify all other SIPRNet systems to use the SIPRNet PKI credential for access control.

More sophisticated access control is possible as the technology enables the linkage of identification with organizational and user roles (e.g., knowing someone is a CENTCOM intelligence analyst). Information services can then make access control decisions "on-the-fly" without having pre-arranged user accounts – the system positively identifies the user's identity, attributes and role. This allows better information access by unanticipated users, and more agility in the way DoD missions are done.

However, it is very important to note that while the technology can provide for very specific access controls, it will be difficult to (1) categorize the many different roles and (2) decide what information should be accessible to users performing in those roles. The technology will make it possible to determine who is accessing what, make it much easier to audit activity, and to control access based on identity and role. However, while this can make it possible to prevent the "financial analyst" from accessing large amounts of intelligence data, the general intelligence analyst or operational planner will still need to have access to enormous amounts of data since such access is essential to successful performance of their function.

Insider Threat Detection

There are a number of working groups dealing with the insider threat problem at the interagency and DoD levels, some predating WikiLeaks, and some formed recently. For example, the National Counterintelligence Executive (NCIX) is leading efforts to establish an information technology insider detection capability and an Insider Threat program – primarily focused on the Intelligence Community. DoD counterintelligence, security and information assurance personnel are engaged in the NCIX insider threat initiatives.

As stated previously, within DoD the Secretary has designated the ASD(HD&ASA) to develop and lead a holistic DoD Insider Threat Program. To create an effective and functional program to protect the DoD, the four primary components - Counterintelligence, Information Assurance, Antiterrorism/Force Protection and Security – must work in partnership; the emerging DoD Insider Threat program will drive that integration. A plan is being developed for a DoD-wide IT audit, monitoring and analysis capability to identify suspicious behavior on all DoD information systems. As an

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000053 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.021

element of the DoD Insider Threat Program, USD(I) has been developing comprehensive policy for a DoD CI Insider Threat Program to detect, identify, assess, exploit and deny insider threats that have a foreign nexus, and that may lead to espionage and support to international terrorism. The DoD CI Insider Threat program activities can also identify other individuals who pose a potential insider threat but are not linked to foreign intelligence services or international terrorist organizations. DoD CI personnel will forward such information to the appropriate officials. Policy for the CI Insider Threat program is in coordination. The Director of DIA, the DoD CI Manager, has taken the functional lead for CI Insider Threat for the DoD CI community. He has directed the DoD Insider Threat CI Group to assist the DoD Components in establishing CI Insider Threat programs, identifying best practices and providing functional guidance.

Our strategy on tools is to examine a variety of Insider Threat detection technologies and employ them where they are most appropriate. One very promising capability is the Audit Extraction Module (AEM) developed by the National Security Agency (NSA). This software leverages already existing audit capabilities and reports to the network operators on selected audit events that indicate questionable behavior. A great advantage is that it can be integrated into the HBSS we have already installed on the network, and so deployment should be relatively inexpensive and timely. AEM is being integrated into HBSS now and will be operationally piloted this summer.

Commercial counterintelligence and law enforcement tools – mostly used by the intelligence community – are also being examined and will be a part of the overall DoD insider threat program. These tools provide much more capability than the AEM. However, while currently in use in some agencies, they are expensive to deploy and sustain even when used in small, homogeneous networks. Widespread deployment in DoD will be a challenge. The Army is working on piloting one of these tools on parts of their intelligence networks and this should give us some good data on cost and utility.

In support of this activity we are employing our Enterprise Software Initiative to put in place a contract vehicle to support acquisition both for existing and future insider threat detection tools. The contract – a basic purchasing agreement – should be in place by June 2011.

Improving Information Sharing and Protection

As DoD continues to move forward with improving our information sharing capabilities, we will continue to concurrently improve our posture and mechanisms to protect intelligence information without reverting back to pre-9/11 stovepipes. DoD is

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000054 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.022

currently involved in multiple interagency level working groups designed to identify specific strategies to improve intelligence information sharing while ensuring the appropriate protection and safeguards are in place. Solving these problems will require a multi-disciplinary, whole of government approach, which DoD is helping solve by conducting a review of our own practices and identifying lessons learned. DoD's mission and extensive experience in dealing with complex sharing issues with foreign and domestic partners provides unique perspectives and will serve as a reference for our plans.

One of the immediate results from these interagency level discussions is the highlighted need for stronger coherence among the various policies governing the dissemination and handling of classified national security information, including intelligence, across the Government. DoD agrees with the DNI that responsible information sharing must include mechanisms to safeguard intelligence while protecting valuable sources and methods. The Department believes this is an inherent responsibility of every individual using the network. This dual responsibility to share and protect information requires a comprehensive approach including coherent policies, responsive architectures, better tools for sharing and protecting, effective training and education, uniform cultural behaviors underpinned with strong, proactive, responsible leadership.

The activities we already have underway to improve information sharing will inherently improve our ability to protect. Increased emphasis on user authentication, data tagging, development of user attributes, and implementation of advanced technologies such as Cloud implementations, consolidated discovery, and single-sign on will provide the foundational technology that will continue to improve sharing and data discovery while bringing protection up to the same level.

Conclusion

The full impact of the WikiLeaks disclosures may not be evident for some time. It is clear, however, that the unauthorized release of U.S. information by WikiLeaks has adversely affected our global engagement and national security and endangered the lives of individuals who have sought to cooperate with the United States. It is of vital importance to DoD and the entire U.S. Government that we keep our sensitive and classified information secure, while at the same time ensuring that the right people have the timely access they need to help keep our country and its citizens safe. We appreciate the Committee's attention to this important issue, and look forward to a continued dialogue as we move forward together.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000055 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.023

Statement for the Record

before the
Senate Homeland Security and
Governmental Affairs Committee

"Information Sharing in the Era of WikiLeaks:
Balancing Security and Collaboration"

Statement of Corin R. Stone
Intelligence Community Information Sharing Executive
Office of the Director of National Intelligence

10 March 2011

Statement of Corin R. Stone
Intelligence Community Information Sharing Executive
before the
Senate Homeland Security and Governmental Affairs Committee
10 March 2011

Introduction

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, thank you for the invitation to appear before you today to discuss the Intelligence Community's (IC) progress and challenges in sharing information. I want to first recognize the Committee's leadership on these important issues and thank you for your continued commitment to assisting us as we address the many questions associated with the need to both share information and to protect it.

Information Sharing

As the IC Information Sharing Executive (IC ISE), my main focus today concerns classified information – and, in particular, information that is derived from intelligence sources and methods, or information that is reflected in the analytic judgments and assessments that the IC produces. I want to be clear, though, that our concern for the protection of information is not restricted to the fragility of sources and methods, but extends as well to broader aspects of national security. We recognize, and will hear today, that the Departments of State and Defense, as well as other federal agencies, themselves originate classified national security information that is vital to the protection of our nation and conduct of our foreign relations, and this information is, like intelligence information, widely distributed and used throughout the government to achieve these objectives. As we have seen recently, the unauthorized disclosure of any form of classified national security information has serious implications for the policy and operational aspects of national security.

I am acutely aware that our major task is to find what the Director of National Intelligence (DNI) has termed the "sweet spot" between the two critical imperatives of sharing and protecting information. To ensure that we share and protect information effectively, we work to find the "sweet spot," as the compelling need for information sharing remains a top priority for the DNI and the IC.

The need is compelling because information sharing is essential to provide quality intelligence support to such disparate activities as coalition warfare, counternarcotics, counterproliferation, homeland security, and cybersecurity. Intelligence judgments and reports that reflect our commitment to sharing information are also essential to support senior policymakers who must deal with matters of increasing complexity in a world that is interconnected and fast-paced. Every day, the talented collectors and analysts within the IC share vital information with each other, our partners, and customers, to provide critical support to senior policymakers across the Executive Branch and Congress. We have made great strides in the post-9/11 era, especially in the counterterrorism mission. The United States is safer because of the progress we have made –

66677.025

as a Community and as a Government – in sharing information more effectively and raising "signals" from the "noise."

Our efforts are not a matter of finding a "balance" between the need to share information and the need to protect; that term implies a "zero-sum" relationship that, as we increase sharing, for example, we also decrease protection. We believe it is more accurate to approach this relationship as one that requires coordinated increases in protecting and sharing information. In other words, as we increase information sharing, we must also increase the protections afforded to that information.

With that approach in mind, we are working to ensure that the IC has the policies, practices, and technologies in place to enable the Community to share information, while both protecting the information and safeguarding privacy and civil liberties. It is clear, for example, that a fundamentally important relationship exists between the parallel needs to share and protect information, and the IC's technology systems and networks' ability to securely store and handle that information. But we also recognize that some of the most complex matters that must be addressed as we increase the sharing of intelligence within and beyond the bounds of the IC largely relate to policy, legal, and cultural issues.

IC Information Sharing Executive

To provide additional emphasis in those areas (policy, legal, and cultural), and to move the center of gravity for the IC beyond technologies and systems, the DNI reassigned the IC ISE role from the IC Chief Information Officer to the ODNI's Office of Policy and Strategy in October 2010. As the DNI's appointed IC ISE, I am developing a coordinated and comprehensive plan for responsibly managing information sharing activities within the ODNI, across the IC, and with all of our mission partners.

To that end, I have established an internal governance process for ensuring a coordinated information sharing approach within the ODNI. I have also refashioned and reinvigorated the IC ISE's engagement activities and governance across the IC to do the same, as well as to set IC-wide priorities and oversee their execution. In carrying out these functions and this mission, I am directly accountable to the Principal Deputy Director of National Intelligence. In addition, I have an excellent partnership with the Program Manager for the Information Sharing Environment (PM-ISE), who focuses on sharing information related to counterterrorism and homeland security across the entire U.S. Government. Our close working relationship helps me ensure that the information sharing activities we undertake in the IC related to those areas are consistent and interoperable with the steps being taken across the entire U.S. Government, as well as with our state, local, tribal, and private sector partners. In this partnership, we agree; responsible information sharing remains our top priority.

Finding the "Sweet Spot"

The IC's work on the complicated questions related to access to intelligence, and the ways in which it can be a shared responsibility, pre-dates the recent unauthorized disclosures. The challenges associated with both sharing and protecting intelligence are not new and have been a

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000058 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.026

factor of major consideration in the Community for years. As this Committee knows all too well, it is one of the foundational principles underlying the Intelligence Reform and Terrorism Prevention Act of 2004, as well as the creation of the Office of the Director of National Intelligence. The latest unauthorized disclosures, however, underscored again the importance of a comprehensive approach to address those challenges.

Working within the broad Government effort that is underway to address the security of classified information in the context of information sharing, the IC's strategy involves three interlocking elements:

- The first is ACCESS: ensuring that the right people can discover and access the networks and information they need to perform their duties, but not to information that they do not need. This is a complex matter that is centered on the principle of determining "Need to Know."

- The second element is TECHNICAL PROTECTION: technically limiting the ability to misappropriate, manipulate, or transfer data, especially in large quantities, such as by disabling or prohibiting the use of removable media on classified networks, including thumb drives and CDs.

- The third area is AUDITING and MONITORING: taking actions to give the IC day-to-day confidence that the information access granted to our personnel is being properly used. This involves monitoring and auditing user activity on classified computer systems to identify anomalous activity, and following up accordingly.

We are also focused on additional measures to protect classified information from "Insider Threats." Consequently, in concert with the three principal elements of our strategy, we must also sustain strong personnel security investigation and reinvestigation programs, ensure that we conduct effective security awareness training, and take or support action against those who disclose classified information without authorization.

Addressing the Insider Threat

The damage caused by the unauthorized disclosures of classified information stems from the actions of individuals and their malicious exploitation of the opportunities available to them in a classified environment. Over the course of our nation's history, there have been spies among us, and the actions of those individuals have demonstrated how a trusted insider "gone wrong" can do grave damage to national security. It is clear that we must be vigilant and proactive in trying to detect, mitigate, and deter this threat.

To meet that challenge, the U.S. Government must have a comprehensive insider threat detection capability. The National Counterintelligence Executive (NCIX) has developed such a program for the IC, and we are working toward implementing its principles. Over the course of the last several months, agencies have worked together to support the development of an insider threat monitoring capability that can be deployed across the entire Government. There are different maturity levels across the Government, and, as a result, improvements will be phased throughout

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000059 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.027

implementation. Technology refresh is a vital part of this program and is being considered for emerging threats, as well as our technology platform, for sharing and protecting information. A robust insider threat detection program will allow departments and agencies to manage the risk caused by granting broader access to sensitive information in Government.

In structuring and implementing insider threat efforts, however, it is paramount that each department and agency ensures privacy protections are in place, and that access to insider threat detection information and activities are limited to authorized personnel performing counterintelligence, security, and other appropriate oversight missions.

It is also important to note that insider threat capabilities are not intended only to detect or deter potential bad actors. These capabilities are also critical to build and increase confidence that access to intelligence is being properly used and protected. That confidence is essential to building a culture that supports responsible information sharing.

Security

Executive Order 13526 established the Information Security Oversight Office (ISOO) of the National Archives and Records Administration as the oversight organization for safeguarding classified information in the federal government, and gave the DNI responsibility for the oversight of all classified national intelligence information. The ONCIX performs the security oversight function for the IC to ensure that its 17 agencies and elements have effective measures and mechanisms to protect classified national intelligence from unauthorized disclosure, and to ensure that any security barriers to information sharing are necessary.

There has not been a unified process to assess the counterintelligence, security, and information assurance postures within all Executive Branch departments and agencies. Departments and agencies currently assess their own performance and compliance with internal programs and regulations. In coordination with OMB, ISOO and ONCIX will evaluate and assist agencies in their assessments, and plan to use on-site reviews as part of that process.

Technology

A dual-pronged approach is needed to improving technology solutions in the classified information sharing environment: (1) enhancements to logical and physical security controls; and (2) incremental delivery of information sharing capabilities through prioritized mission needs from the intelligence, defense, and civilian agency communities.

Critical capabilities supported by technology – such as identity and access management, data protection and discoverability, and a reliable audit process – play an integral role in the steps we are taking to find the "sweet spot" between the need to share and the need to protect intelligence. In particular, technology can help regulate the availability of information. It can also help to identify and prevent the potential misappropriation, manipulation, or transfer of data; as well as the means by which such actions can be taken. Further, technology can record users' actions and

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000060 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.028

support the investigation and prosecution of those who intentionally misappropriate classified information. The IC is working to provide end-to-end data management technology to ensure that sensitive intelligence data is appropriately protected throughout its life cycle (creation, use, transit, storage).

To enable strong network authentication and ensure that networks and systems can authoritatively identify who is accessing classified information, the IC CIO is implementing user authentication technologies and is working with the IC elements to achieve certificate issuance to eligible IC personnel in the first quarter of fiscal year 2012. In addition to networks and systems, the IC is working to advance the authentication standards to applications in order to better protect data. Identity management for both networks and applications represent the foundational capability required to enable access management decisions and ultimately the recording or audit of users' actions with attribution.

The IC plans to increase access control to critical IC information resources, based on Data Protection Models in fiscal year 2011-2012. To that end, the IC CIO is standardizing a Data Protection Model based on current and evolving protection requirements and identity attributes. This approach will allow for several levels of protection; from open access through highly restricted availability. The appropriate protection level will vary based on factors such as data sensitivity, environment, mission criticality, and systems capabilities. Important elements in this approach include authentication techniques and the use of attributes (such as clearance level) to determine identities and support mission-based access to intelligence. Access control capabilities ensure that information content is only accessible by those individuals who possess the appropriate need, as validated by their management.

For higher levels of protection, technology can be used to control usage and limit user capabilities to perform activities such as copying, printing, or exporting data to a device. At this level, access requires strong user identification and authentication for system access along with the use of one or more attributes such as clearance level, digital identifier, role, or Community of Interest.

Data discoverability is another vital component to enable sharing while appropriately restricting access to information content. In the event that a user is inadvertently denied access to information needed to perform the mission, yet does not possess the appropriate attributes (for example clearance level, organization, or "Need to Know"), this capability will allow that user to discover the existence of, and request access to, the information

Finally, audit and monitoring technologies are necessary to ensure that employees' access to intelligence information is recorded and anomalies are detectable. Implementation of audit and monitoring technologies, by providing a reliable record of users' actions, will support our ability to identify and react to apparently inconsistent activities, while also affording a means of deterring errant user behavior. During fiscal year 2012, the IC CIO will leverage an Enterprise Audit Framework to enhance the sharing of audit data across the IC elements.

In addition to these critical technologies – identity and access management, data protection and discoverability, and a reliable audit – the IC CIO continues to look at ways to leverage additional

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000061 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.029

technologies, such as digital management and data loss prevention, to find the "sweet spot" between sharing and protecting intelligence.

Conclusion

The IC is fully committed to giving policymakers, warfighters, law enforcement officers, and our other partners the best intelligence and analytic insight we can provide. This support is essential to enable all those we serve to make the decisions, and take the actions that will protect American lives and American interests, here and around the world.

To carry out that critical mission, it remains vitally important to both share and protect networks, intelligence, and associated information – and the systems and networks that support them. As we continue to increase sharing, we must also increase the protections put in place to heighten confidence that the intelligence and information that is being shared is being properly used and protected. This is a matter of managing risk; and people, policies, processes, and technology all play important and interconnected roles in managing that risk.

Appropriate policies must be aligned across many information sharing constituencies to include, federal, military, state, local, tribal, private sector, and international partners. These policies must also be consistent with the law, and appropriately address civil liberties and privacy concerns. Cultural attitudes and behaviors must reflect these priorities, and be shaped through appropriate training and incentives. Work on the next generation information sharing environment must begin now and be collaboratively developed with the IC and other stakeholder agencies.

Whether classified information is acquired via a computer system, a classified document, or simply heard in a briefing or meeting, we have had "bad apples" who have misused such information before and, unfortunately, we will see them again. That does not mean we should err on the side of not sharing intelligence or information – the risk caused by not sharing the information we have with those who need it is simply too great. Rather, we must put all proper safeguards in place, continue to be forward leaning to find the threat before disclosures occur, be mindful of the risks, and manage those risks in the light of the importance of our mission.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000062 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.030

Statement for the Record

before the
Senate Homeland Security and
Governmental Affairs Committee

"Information Sharing in the Era of WikiLeaks:
Balancing Security and Collaboration"

Statement of Kshemendra Paul
Program Manager for the Information Sharing Environment

10 March 2011

Statement of Kshemendra Paul
Program Manager for the Information Sharing Environment
before the Senate Homeland Security and Governmental Affairs Committee
10 March 2011
"Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration"

Introduction

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, thank you for the opportunity to speak about our efforts to effectively share and protect information at every level of government. I want to thank the Chairman and Ranking Member for their attention to information sharing reform efforts and support of my office's mission. I also recognize my fellow panelists who are key partners in our government-wide efforts to further strengthen information sharing and protection.

As the WikiLeaks story emerged, concerns were voiced that information sharing efforts would suffer a setback. This Administration is committed to improving information sharing and information protection. While complex and challenging, we do not see a conflict between these goals. Guidance throughout the Executive Branch has been consistent: we need to continue to accelerate our information sharing in a responsible and secure way. As has been echoed by Chairman Lieberman and Ranking Member Collins,[1] Secretary of Defense Gates, Office of Management and Budget Director Lew, and Director of National Intelligence Clapper have each championed efforts to further strengthen information sharing and protection; what Director Clapper has termed the "sweet spot" between the two.

The WikiLeaks disclosures primarily involved classified information, but the fundamental challenges associated with sharing and protecting sensitive information span across all security domains, including classified and sensitive but unclassified domains. Moreover, missions do not stop at the security domain or at organizational boundaries. Fundamental policies and solutions

[1] Wall Street Journal, Op-Ed, Dated: January 26, 2011.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000064 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.032

should be framed to address all types of protected information, classified and unclassified, held by the federal government and by our state, local, tribal, private sector, and international mission partners. Across all mission partners, no matter the level of government, we need to establish structural elements such as strong governance, strategy, and policy to move incentives towards common, comprehensive solutions and away from agency-based, bilateral, fragmented approaches.

Information Sharing Environment[2]

My role, as outlined in the Intelligence Reform and Terrorism Protection Act of 2004, is to improve the sharing of terrorism-, homeland security-, and weapons of mass destruction-related information sharing across the federal, state, local, and tribal governments, as well as with the private sector and international partners.[3] I co-chair the Information Sharing and Access Interagency Policy Committee, which integrates the Information Sharing Council with the National Security Staff Senior Director for Information Sharing Policy.

The Information Sharing Environment facilitates sharing at all security domains among federal agencies, and across all levels of government. Our mission partners own the Information Sharing Environment. As you know, the Information Sharing Environment is defined through both a vertical mission – terrorism, homeland security, and weapons of mass destruction information sharing – and through a number of desired attributes,[4] a horizontal, cross-cutting, data-centric information sharing and protection capability. The law granted the Program Manager government-wide authority – a unique capability allowing us to work with existing programs to facilitate assured information sharing.

---

[2] For more information, see www.ise.gov.

[3] IRTPA, as amended, Section 1016

[4] IRTPA, Section 1016(b) (2) (I), for example, requires "strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls".

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000065 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.033

The Program Manager's role is to plan for, oversee the agency-based delivery of, and manage the Information Sharing Environment. Our office is not operational; agencies conduct mission operations, agencies develop and implement policy and procedures, and agencies make investments to interconnect systems, networks, databases, and business processes. Collectively, these contributions by mission partners form the Information Sharing Environment.

A practical way to think of the Information Sharing Environment is as an infrastructure and capability – analogous to the interstate highway system. The Information Sharing Environment represents the structure and "rules of the road" – including commonly understood road signs, traffic lights, and speed limits – that allow information traffic to move securely, smoothly, and predictably. We are charged with ensuring that the Information Sharing Environment is built to improve sharing and protection of terrorism, homeland security, and weapons of mass destruction information. If built properly, everyone can use the roads within appropriate mission and policy context. Indeed, like other infrastructures, the Information Sharing Environment is a public good and has the potential to pay dividends by supporting information sharing and protection beyond its initial mission space. Terrorism-related information can flow between partners, as can other classes of information such as those related to non-terrorism intelligence and law enforcement.

The law does not ask my office to do this alone – we are not pouring the concrete – rather, we are providing leadership and coordination of a complex set of factors that make the highway safe and navigable: governance and engagement, strategy and policy alignment, business process harmonization, guidelines, standards, and architecture. This leadership and coordination enables our mission partners – the general contractors building and managing the day-to-day operation of the highways – to build to common specifications.

In the five years since Congress directed the creation of the Information Sharing Environment, significant steps have been taken toward establishing a strong foundation. Important mission initiatives, such as the Nationwide Suspicious Activity Reporting Initiative, and core capabilities

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000066 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.034

and enablers, such as the National Network of Fusion Centers and the National Information Exchange Model, have produced results and show ongoing promise. Yet, as the persistent and evolving threat demonstrates, including vulnerabilities underscored by the WikiLeaks breach, much more remains to be done.

Information Sharing and Protection Opportunities

The WikiLeaks breach is not principally an information sharing problem; at its root a bad actor allegedly violated the trust placed in him. While we cannot always stop bad actors, we can take this opportunity to reassess our posture, our progress, and our focus regarding information sharing and protection to take a more holistic approach. When examining the full scope of information sharing and protection, there are many widespread and complex challenges that must be addressed and solved by multiple agencies and organizations together. The insider threat, the security concerns, and related challenges are being tackled by our mission partners – as described by my fellow panelists. Many of the best practices and work being done by our mission partners can, and should, be scaled more broadly.

From the lens of the Information Sharing Environment, we have observed three opportunities from the WikiLeaks incident that we believe require attention. First, a **whole-of-government** approach is necessary to effectively address these issues in a robust way. Second, fundamental policies and solutions should be framed to address all types of protected information, **classified and unclassified**, held by the federal government and by our state, local, and tribal partners, as our critical national and homeland security issues cut across security domains. Finally, a strong and broadly applied **governance, strategy, and policy framework** is foundational to improving information sharing and protection. A strong, comprehensive governance framework will help streamline policy and standards across the federal government.

We are being deliberate and collaborative in our approach. My office is currently leading an effort to update the 2007 National Strategy for Information Sharing. As part of this effort, we are reviewing the post WikiLeaks-related developments to determine how best to incorporate

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000067 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.035

improvements to both sharing and protection, and are engaged with our mission partners and other stakeholders to understand their needs, requirements, missions, and opportunities. As we further refine the principles of the strategy, the end goal is to accelerate the development and implementation of the Information Sharing Environment and contribute to our government's ability to securely and effectively share terrorism, homeland security, and weapons of mass destruction information among our mission partners.

Today, the mission spans organizational boundaries. It is only possible to further strengthen information sharing and protection by supporting these cross-cutting missions through shared policies, guidelines, and common standards; accompanied by governance, training, logging and auditing, performance management, and oversight mechanisms that provide confidence and accountability spanning all mission partners. No one size fits all, but an ecosystem that allows for effective risk-based decisions ensures progress.

Activities

We, in coordination with our mission partners, are actively working on a number of initiatives which will reduce the risk of another WikiLeaks–like incident. We want to build on current momentum to accelerate delivery of the Information Sharing Environment to provide a trusted, assured information sharing and protection ecosystem. The following demonstrate our work with both mission partners and with industry to develop and provision the standards-based Information Sharing Environment:

- **Harmonizing protection policy**. Robust privacy and security protections are critical to an effective Information Sharing Environment. The capabilities that permit policy-driven, predictable, mission-effective, and efficient information sharing are similar to the capabilities that increase privacy and security.
- **Driving Assured Interoperability across our Sensitive but Unclassified and Secret Networks.** The Program Manager for the Information Sharing Environment is supporting mission partners to deliver assured sensitive but unclassified network interoperability and assured secret network interoperability. Efforts regarding the

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000068 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.036

sensitive but unclassified networks are focused on the Federal Bureau of Investigation's Law Enforcement Online; the Department of Justice's grant-funded, state-owned Regional Information Sharing System Network; the Department of Homeland Security's Homeland Security Information Network; and the Intelligence Community's Intelink. The assured secret network interoperability effort brings together eight agencies[5] that operate at least 10 distinct secret networks with three main goals: (1) to streamline and ensure effective mission and policy framework for sharing classified information with our state and major urban area fusion centers; (2) to enhance governance and multi-lateral decision making to replace the current patchwork of bilateral agreements, and (3) to enhance operational coordination.

- **Harmonizing the Various Identity, Credential, and Access Management Frameworks.** There are at least five identity, credential, and access management frameworks in use by federal agencies.[6] These frameworks are critical to establishing trusted, assured identity, which in turn is foundational to information sharing and protection. It is essential that these frameworks are interoperable. While there is a large degree of bilateral alignment, the risk of fragmentation remains. The Program Manager for the Information Sharing Environment is focused on this challenge and is stepping up efforts to characterize necessary distinctions while focusing on shared minimum capabilities and whole-of-government optimization.

- **Reinventing the Public Safety Business Model.** The Information Sharing Environment's flagship initiatives, in conjunction with mission partners, have had a counterterrorism and homeland security focus, such as the network of state and major urban area Fusion Centers and the Nationwide Suspicious Activity Reporting Initiative. The Department of Homeland Security's Law Enforcement Information Sharing Service, the Federal Bureau of Investigations' National Data Exchange and the state-owned

[5] Office of the Director of National Intelligence, Department of Defense, Department of Homeland Security, Department of State, Department of Treasury, Department of Energy, Department of Justice, and the Federal Bureau of Investigation.
[6] These include: the Federal CIO Council's Federal Identity, Credential, and Access Management (FICAM) Roadmap and Interoperable Personal Identity Verification (PIV-I) guidance for unclassified networks; the Department of Justice's Global Federated Identity and Privilege Management (GFIPM) standards for unclassified networks and non-federal partners; DOD's Committee on National Security Systems PKI for secret networks; State Department, FBI, and Justice PKI solutions on their individual secret networks; the Intelligence Community's Identity and Access Management (IDAM) effort across all IC networks at all security domains.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000069 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.037

National Law Enforcement Telecommunications System, or Nlets, highlight related and aligned national-scope law enforcement solutions. For our state, local, and tribal partners, counterterrorism is an important mission, but it is only one facet of the overall mission of protecting the American people. By advocating for, and embracing, an integrated, all-crimes, all-threats, all-hazards approach, all of our mission partners are positioning themselves to apply the broad benefits of the Information Sharing Environment to their entire mission. Our domestic mission partners are also looking at how to respond to a constrained budget environment by enhancing coordination and shared services across jurisdictions and levels of government through leveraging core Information Sharing Environment frameworks, policies, guidance, standards, and architecture.

- **Adopting Information Exchanges.** Two of the most important initiatives that must be implemented to enable effective information sharing are: (1) standardizing and translating terminology, code lists, and data definitions; and (2) harmonizing business processes so that all mission partners have a context for standardized information exchanges. To solve this issue, the National Information Exchange Model allows disparate systems to share, exchange, accept, and translate information. The National Information Exchange Model has been adopted by 13 cabinet agencies, is used internationally, and has been endorsed by the National Association of State Chief Information Officers. The required use of the National Information Exchange Model has also been incorporated into federal grant guidance issued by the Department of Homeland Security and the Department of Justice. The use of this framework enables greater information sharing through the use of existing exchanges and policy automation and enforcement through enterprise standards for security, access, and data protection.

Another key activity for solving these challenges rests in aligning and strengthening a comprehensive governance and outreach framework – a core focus of our office. There are three components to the current governance and outreach structure:

- Intergovernmental policy development, the first tier, represents the top-down authoritative source of direction for driving innovation by developing information requirements and defining mission processes through harmonizing common mission

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000070 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.038

equities. This is accomplished primarily through the Information Sharing and Access Interagency Policy Committee, its five subcommittees, and related working groups, where interagency policy decisions are discussed and made.

- The second tier is bottom-up, bringing the voice of the practitioner and subject matter experts to a collective table. To promote information sharing, existing representative organizations or intra-agency bodies are leveraged to promote collaboration for functional requirements and standards, to engage the key information integrators and best practices, and to promote seamless information sharing and protection.
- The third tier is outside-in, providing a means for mission partners to effectively communicate and collaborate with industry. The architecture, methodologies, and technologies used to build the Information Sharing Environment will rely upon standards that must be developed based on shared mission partner requirements.

Additionally, we are actively working with our interagency partners to develop further recommendations for how to enhance protections and improve information sharing. We are following agency reactions to WikiLeaks to ensure information protection efforts do not set back recent information sharing improvements or impede future information sharing improvements. As we work through these efforts, we will keep you informed.

Conclusion

In closing, pursuant to our charter in law, our efforts have been and, continue to be, focused on information sharing in a responsible and assured manner. We are committed to advancing the sharing of information with the protection of information. Effective information sharing and collaboration are absolutely essential to keeping America safe. The risk of future WikiLeaks-like incidents can be reduced; but, fixing these government-wide challenges is complex, difficult, and requires sustained commitment. We are committed to further strengthening information sharing and protection together. Thank you for your continued support and guidance as we work together on solutions to implement this critical national security priority.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000071 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.039

Written Testimony of Thomas E. McNamara
Committee on Homeland Security and Governmental Affairs
Thursday, March 10, 2011
Dirksen Senate Office Building – SD 342

I am Thomas McNamara and from early 2006 until late 2009 I served as the Presidentially appointed Program Manager for the Information Sharing Environment, which position was administratively located in the Office of the Director of National Intelligence, but whose statutory authorities and mission extend beyond the Intelligence Community to the entire federal government. It is again a pleasure to testify before this committee. During my years as Program Manager, I had nothing but understanding, encouragement, and bipartisan support from the committee. For that, I thank the committee and especially the Chair and the Ranking Member.

During that time, I directed a very broad effort to design, create, and develop the sharing of terrorism-related information among Federal, State, local, tribal and foreign governments, and with the private sector. Congress established the PM-ISE specifically to address deficiencies identified by both the 9-11 and WMD commissions by mandating the creation of an Information Sharing Environment (ISE) to ensure that those responsible for protecting our nation from future terrorist attacks have the information they need to be effective.

I need not, and will not, go into detail here to redundantly describe the ISE or the Program Manager's Office to this committee. For those few others who might read this statement, let me note for the record that the Information Sharing Environment (ISE) has been built with the objective of sharing the right information with the right individuals at the right time. This can only happen through balanced ISE access and control mechanisms, which are well known, and already widely used in the private sector.

In my last appearance before this committee, I noted that we had built a strong foundation for the ISE, but that a fully functional and mature ISE was still a desideratum. The Wikileaks disaster is an unfortunate confirmation of the truth of that evaluation. Let me try to convey my understanding of the circumstances that gave rise to the Wikileaks disaster. I base these observations entirely on unclassified sources, having had no access to classified information regarding Wikileaks, or of any events, since my departure from government service in 2009.

First, a truly mature and fully functioning ISE can only occur when we establish rationalized, standardized, and harmonized rules, procedures, and operating systems, without which we cannot manage the ISE. To get from the start point in 2005 to that fully mature system is a long, complex, and difficult process. We are, I believe, well along the path, but we have not, by any means, reached our goal. The foundation is there, and the goal was articulated in the 2006 Implementation Plan, and the 2007 National Strategy for Information Sharing Environment. As we progress in our endeavor, we need to modify and update those documents to refine and clarify our understanding of that goal.

We have rational plans and a strategy in those documents for reaching our goal of a mature ISE. But, we have not finished creating the standardized and harmonized rules, procedures, and operating systems that we need. That incomplete standardization and harmonization are the reasons for the Wikileaks disaster. The case is one where two agencies had two different ideas of how to manage the same information. Had there been standardized and harmonized rules, both agencies would have known how this information should be managed, and had confidence that the other was managing it properly. In this post-1990s information world, the government no longer has the option of letting each agency manage, as it wishes, the information of which it is a custodian (not an owner). Managing information in the 21st Century is a common enterprise.

66677.040

Here are, in my opinion, some of the major ISE-related problems that allowed Wikileaks to occur. [I will cite one fundamental, non-ISE-related problem at the end of my remarks.]

1. The ISE was never envisaged to give very broad access to information in systems where control mechanisms are inadequate to ensure that only the right information flows to the right people at the right time. Such controls are accomplished, as mentioned above, through standardized rules, procedures, and operations, including adequate auditing and monitoring, and some form of authorized-use. Unfortunately, they were not in place on SIPRNet. SIPRNet tends to have very restrictive controls in place for non-DoD personnel, but allows wide-ranging, non-job-related access to information for hundreds of thousands of Defense Department employees. Two misconceptions that plague many agencies' thinking about information sharing are apparent in DoD's management of SIPRNet. The first is that an agency's own cleared employees are more reliable and need fewer restrictions than another agency's cleared employees. The second is that an agency's "own information" is more tightly controled than other agencies' information.

2. In the aftermath of the Afghanistan and Iraq invasions, a very high priority was placed in DoD on getting to the "war fighters" all the information they might need to get their jobs done – i.e. to fight the wars. This necessary and laudable objective relied on SIPRNet as the main network for moving secret information to war fighters in combat zones. The effectiveness of SIPRNet controls diminished, *inter alia*, because of the reduced capabilities for auditing and monitoring SIPRNet in the Iraq and Afghanistan theaters of operations. The priority of getting information to the war fighters was the justification for the relaxation of rules. One of the mistakes in the SIPRNet control system in combat zones is that large volumes of information transfers – i.e. "mass data downloads" – were permitted so that information could rapidly move to the war fighters, even without auditing and monitoring capabilities, which would have been used in a fully developed Information Sharing Environment.

3. In recent years government and private industry have placed increasingly stronger restrictions on the transfer of data to portable storage devices (e.g. thumb drives, disks, PDAs). Most controlled systems prohibit using uncontrolled portable storage devices to move data within and between information systems. Within SIPRNet these controls were not in place, or not used, in Iraq and Afghanistan, thus, allowing the transfer of classified information to unclassified systems with little or no auditing, or monitoring of the transfers.

These three problems are three lessons to learn from the major WikiLeak affairs of the past year (the Afghanistan messages; the Iraq messages; and the State Department messages). The information sharing environment cannot survive without fixing these failures by establishing rationalized, standardized, and harmonized rules, procedures, and operating systems across the federal government.

WikiLeaks is a case of information sharing outrunning the system used to manage the shared information. The statement, "there can be no sharing without security," is as true today as it was the day I began as Program Manager. Successful information sharing involves not only the sharing, but also the secure management of the information and the environment in which information is flowing. Much of the misunderstanding of the ISE, and of failures such as the WikiLeaks, comes from sharing when the systems cannot manage the volume and sensitivity of the information.

It has been a constant theme of mine, and others whobuild the ISE, that two groups of stakeholders in the ISE must be satisfied. The first is the participants, the information users. They will not use the ISE unless they have confidence that the system will properly control and protect the information that they put into it. The second is the non-participants, i.e. mainly the American public, and others who have a major

66677.041

stake in the proper functioning of the ISE. They will oppose any ISE that cannot control and protect the privacy of information that pertains to them. The confidence and comfort of both groups must be satisfied, or the ISE will not succeed.

While attention is on the WikiLeaks affair, I want to point out that these problems are not just problems for classified information, i.e. for sensitive national security information. An even greater volume of sensitive information is unrelated to national security, and therefore, cannot be classified. I refer here to the huge category called Controlled Unclassified Information (CUI). This category requires its own rationalized, standardized, and harmonized controls because it concerns law enforcement, judicial, private-sector proprietary, personal, and much other sensitive information.

It is not hard to imagine an individual with access to CUI information downloading and releasing large quantities of data about, for example, grand jury deliberations, or organized crime investigations by local, state or federal law enforcement. Indeed, there is much CUI contained in the WikiLeaks documents. Hence, very early on, as Program Manager, I zeroed in on the chaotic state of sensitive but unclassified (SBU) information. We created CUI as a rationalized, standardized, and harmonized method within the ISE for managing this information across the federal government. We, also, made it adaptable for use by state and local governments. This CUI management is an essential part of the ISE, and is coordinated by the National Archives and Records Administration with oversight and assistance by the Program Manager's Office. It is another part of building a fully functional and mature ISE.

I want to take this opportunity to point out, again, to this committee and the Congress an anomaly in the building of the ISE. The legislative mandate for the Program Manager is to build the ISE for "terrorism-related" information only. We can all see that most of the documents in the WikiLeaks were not terrorism-related. Therefore, they were not documents that came under the ISE manadate. Although the Program Manager only has authority for managing terrorism information, no agency partitions off terrorism information from its overall management of all classified or CUI information.

This is why, when I served as Program Manager, I deliberately designed the ISE so that it could serve as an information management system for all classified and all CUI information. That reflects my conviction that it is impossible, and undesirable, to create a "Terrorism-only" ISE. The mission, therefore, is to create a comprehensive ISE, and the mandate and authorities should reflect that mission.

To correct this anomaly, I urge this committee and the Congress, in consultation with the executive branch, to examine this and consider expanding the authority of the Program Manager, or creating a National Executive for Information Management. Such a change will increase the ability of the senior information management official truly to manage all aspects of the ISE.

Nevertheless, when the Departments of State and Defense agreed on the arrangements for DoD access through SIPRNet to State's classified cable traffic, there was no role for, and no consultation with, the Program Manager's office. The practice was that interagency arrangements were the sole purview of the involved agencies. Thus, whatever benefits the experts in the Office of the Program Manager might have added were lost. I do not know if this would have changed the outcome; I simply note that no consultation took placed.

I will conclude with two points. First, it is a measure of the very profound changes of attitudes in government regarding information sharing that no one has called for an end to information sharing because of the WikiLeaks. Had WikiLeaks happened 4-5 years ago, there would have been numerous demands to close the ISE and the Program Manager's office. In fact, even without WikiLeaks, there were such calls back then.

What has happened, I believe, is that we have all seen the absolute necessity of managing information in the new information age, using policies and procedures that respond to the needs of the new age. We may pine for the "good old days," but we can never go back to them. There is simply too much information and too many organizations and individuals requiring information to think government can function properly without an ISE. The rest of our society has moved with alacrity into this new information-sharing world. Government must follow.

Finally, we need to recognize that at its base the WikiLeaks affair was not a new phenomenon. It was in fact a very traditional espionage affair, which used new tools for the espionage. The parallels with other traditional espionage disasters of the past two decades are many. One example is the John Hanson espionage affair. That was also a case of document theft by a cleared, trusted individual, who turned over hard copies (instead of digital copies). Hanson's criminal acts over many years were similar to the criminal acts of the thief who stole and handed over to WikiLeaks, CDs and thumb drives full of sensitive information. In both cases, the acts were meant to undermine the nation's security and weaken our society, even if it meant that people's lives were at risk, and some would be killed.

My point in raising this here is to say that, even without the ISE, we had a John Hanson. And, with an ISE we had a WikiLeaks traitor. As long as trusted individuals debase themselves and betray our trust, there will be Hansons and WikiLeaks. The fully functional and mature ISE, which I have referred to here, is a necessity in this new information age because it is an essential part of our efforts to prevent or limit these disasters in a future, where computerized data flows are the norm, and where human treachery will always be a possibility.

66677.043

Testimony on Behalf of the Markle Task Force on National Security in the Information Age

US SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE

Hearing on Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration

MARCH 10, 2011

Mr. Chairman, Senator Collins, thank you for holding this hearing and dedicating your time and energy to the critical issue of information sharing. And thank you for inviting the Markle Task Force on National Security in the Information Age to submit written testimony in order to help inform the current discussion. You have led this effort since the attacks of 9/11 with a singular commitment to making this nation safer. Since 2002, the Markle Task Force has provided policymakers, including this Committee, with recommendations[1] to help accelerate our government's use of information and information technology to better understand the threats we face and make better decisions about those threats. Our ultimate goal has been to help enable the federal, state, and local governments to work together to protect our nation from terrorism and other threats.

A substantial change has occurred throughout government in the way security professionals do business. Information sharing has become more widespread and the government has made some real changes necessary to respond to new threats. That said, progress has been too slow in some places and has lacked adequate guidance or oversight in others. In light of the recent series of releases of sensitive and classified documents, this progress in sharing information between and among government agencies may be reversed. In October—before the most recent release of the Department of State cables—Director of National Intelligence Clapper observed that the release of classified information by WikiLeaks may have a "chilling effect" on information sharing.[2]

We believe that the government must devote serious attention to preventing further leaks. Policies to control access to information in the Information Sharing Environment are not adequately developed and

---

[1] For more information on all of our previous work on information sharing, please visit www.markle.org/national-security.

[2] Jason Ryan, "President Obama and Intelligence Director Angered Over Media Leaks," *ABCNews*, 6 October 2010, available at http://abcnews.go.com/Politics/president-obama-intelligence-director-angered-media-leaks/story?id=11817252 (last visited 1 March 2010).

66677.044

inadequate audit tools are in place. The government uses both policy and technology correctly in certain arenas, but for years we have urged stronger action across government, led from the top. Nevertheless, efforts to reduce the sharing of information would be misguided and potentially a risk to our national security. Our government has improved how it operates since 9/11, and this improvement needs to be encouraged and sustained. We agree with the statement you, Senators Lieberman and Collins, made in your recent Wall Street Journal op-ed that "...a return to the pre-9/11 era, when agencies hoarded information, would compromise our national security."[3]

Indeed, efforts to reduce information sharing between and among government agencies and the private sector would not only compromise our national security; these efforts might also reduce the public's confidence in other government information sharing programs such as those necessary for the development of health information exchange and the smart grid. The success of these programs, which promise tremendous cost savings, quality improvements, and efficiency gains, is critical for modernizing government and private sector operations and building the foundation for continued innovation and growth in the information economy.

The Need for Information Sharing

The attacks on 9/11 showed all of us that the Cold War "need to know" system for managing classified and sensitive information drove a culture of information security that resulted in countless stovepipes of information and secretive pockets of the nation's most valuable information. This system did not keep America safe in a world of asymmetric threats. Many realized that protecting America in this new threat environment would require the government to operate in an entirely new way.

You have enacted two major laws that have substantially changed how government understands those who would do us harm and how it acts to prevent that harm. We have tried to contribute to this same challenge. Over the course of four reports written between 2002 and 2009[4], the Markle Task Force grappled with how the government could operate in a new way. With national security experts from every administration since President Carter, civil liberties advocates, information technology executives, academics, and many from within government and the intelligence community, we proposed a collaboration across agencies that would foster a robust sharing of information and ideas. This collaboration, to be successful, required a set of policies that would simultaneously empower and constrain government officials by making clear what collection, analysis, sharing, and uses of information were permissible, and what were not. Instead of storing data centrally, we suggested storing data on a distributed network, thus eliminating the gaps between government agencies and empowering all players in the network—including those at the edges—to create and share actionable and relevant information.

---

[3] Joseph I Lieberman and Susan M. Collins, "How to Prevent the Next WikiLeaks Dump," *The Wall Street Journal*, 13 January 2011, available at http://online.wsj.com/article/SB10001424052748703779704576074340363346676.html (last accessed 7 March 2011).

[4] All Markle Task Force reports are available at http://www.markle.org/national-security/publications-briefs-national-security.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000077 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.045

The objective of this network was to enhance the government's ability to discern indicators of terrorist activity amid overwhelming amounts of information, and to create more time for the nation to respond to threats more effectively.

Since 9/11, there has been a shift in federal and state government culture towards this type of information sharing and collaboration model, and some segments of the government have made progress implementing information sharing policies. Government sources indicate that this approach, in turn, has been very successful. In 2010, for example, the Obama administration claimed twenty-two counter-terrorism successes that resulted, in part, from increased information sharing.[5] These successes included charging fourteen individuals with terrorism violations for providing al Shabab with money, personnel, and services; arresting Farooque Ahmed for plotting to bomb Metrorail stations in the Washington, DC area; and discovering and disarming multiple bombs on cargo planes bound for Chicago. The agility that sharing information has given our government officials has enabled them to better understand our rapidly changing world. If information sharing policies and practices had not been implemented, these recent successes might have been tragedies. Clearly, now is not the time to turn back the clock on information sharing.

Of course, there are risks inherent in sharing more information, but these risks are outweighed by the risks of not sharing. The attacks on 9/11 illustrate a stark example of this.

The Breach

Public sources indicate that the recent information breach to WikiLeaks, allegedly committed by PFC Bradley Manning, apparently occurred primarily because of a lack of appropriate policies and technologies that limit the risks of increased access to sensitive and classified information. PFC Manning described the situation he encountered when he downloaded 1.6 gigabytes of classified US government data onto re-writable compact disks: "Weak servers, weak logging, weak physical security, weak counterintelligence, inattentive signal analysis . . . A perfect storm."[6]

The security breach was not an inevitable result of information sharing. We do not have access to any information other than that which has been published in the media, but it appears that the breach was the result of the lack of adequate controls about access to information.

Instead of reducing information sharing, the government should work to minimize the risk that unauthorized disclosures occur by building government-wide authorities and constraints into all

---

[5] Prepared Remarks of John Brennan, Director of National Intelligence, to the White House Press Corps, "Fact Sheet on Security Enhancements: Statement by John Brennan on Holiday Security," 22 December 2010.

[6] "Bradley Manning, in his own words: 'This belongs in the public domain,'" *The Guardian*, 1 December 2010, available at http://www.guardian.co.uk/world/2010/dec/01/us-leaks-bradley-manning-logs (last visited 1 March 2011).

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000078 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.046

information sharing policies and systems. We have counseled greater urgency in this area for many years.[7] As we develop the capability to better share information, we need at the same time to develop the regulations, processes, and use of technology that control access and use.

Authorities and Constraints

Much of the intelligence community and many in other agencies charged with national security have embraced the objective of collaborating across agency lines and sharing more information with those who need it to fulfill their mission. However, the February 2011 GAO report on "high risk" government programs noted, "The government has continued to make progress during the past two years in sharing terrorism-related information among its many security partners, but does not yet have a fully-functioning Information Sharing Environment in place."[8] Implementation of information sharing programs has been uneven across agencies and has not been driven by a government-wide vision of the authorities and constraints necessary to build an effective and trusted information sharing environment.

An essential element of an information sharing environment is that prior to making information available to a wide community, the government should have regulations and processes for controlling access to and use of shared information. Instituting these mechanisms is a critical step in the effort to shift how the government does business. These mechanisms include a standard of authorized use and immutable audit logs. Together, these tools can both prevent unauthorized disclosure of information and help build confidence in the Information Sharing Environment.

Authorized Use[9]

In our third report, *Mobilizing Information to Prevent Terrorism: Accelerating the Development of a Trusted Information Sharing Environment*, we proposed the adoption of a standard of "authorized use" that would enable an individual trying to access information so that they could pursue an area of inquiry to document why they were authorized to use it. In the 2007, 9/11 Commission Recommendations Implementation Act, Congress asked the executive branch to advise whether it thought such a standard was practical. In his March 2008 "Feasibility Report" to Congress, the Program Manager for the Information Sharing Environment (PM-ISE) discussed numerous potential obstacles that he viewed as

---

[7] Previous Markle testimony is available at http://www.markle.org/national-security/publications-briefs-national-security.

[8] GAO, "High Risk Series: An Update," (Feb. 2011), p. 96, available at http://www.gao.gov/new.items/d11278.pdf (last visited 1 March 2011).

[9] More information on Markle's previous work on authorized use is available at www.markle.org/sites/default/files/20090825_authusestndrd.pdf.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000079 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.047

limiting the feasibility of implementing an authorized use standard.[10] None of the objections cited in the report, however, were technical in nature. Commercial, off-the-shelf technology, which continues to become more widely available, enables the use of such a standard even in today's environment of multiple and differing authorities and standards across the government. Again, we believe this standard should be considered.

The authorized use standard, as conceived of by the Markle Task Force, was intended to change information sharing practices in four ways:

1. Information sharing would be based on the specified mission of the receiving office or individual. The threshold question would be whether the requesting agency could articulate a purpose for which the information would be used that was within the specific and authorized mission of that requesting agency. With proper implementation of permissioning systems, that authorized purpose could be specific to a work unit or individual, working a specific problem or threat. The authorized use concept demands clarity of authorized uses; that is, careful consideration of appropriate roles and missions of different agencies, offices and individuals. In our view, it would not be sufficient to claim something as general as "counter-terrorism" or "counter-proliferation" as an authorized purpose. Instead, an authorized purpose would have to be something quite specific, such as "tracing the flow of terrorist financing through the international banking system" or "examining the role of North Korea in the proliferation of nuclear weapons technology."

2. The question of deciding how the information would be used would be based on that objective definition of the mission of the requesting office or individual, rather than the subjective determination by the originator of the requesting entity's "need to know." The originator might still be able to dispute the requesting entity's claim that it had an authorized purpose that it intended to use the information for, but the presumption would be in favor of sharing in response to claims for specific authorized uses, and the adjudication of sharing disputes would be based not on the originator's assessment of need to know but on the adequacy of the asserted authorized use. The concept recognized, of course, that certain information might still not be sharable for security reasons even if an otherwise legitimate authorized use was asserted.

3. Even with clear and consistent guidelines for information sharing, disputes will inevitably arise. Information sharing participants, particularly in the early stages, will confront unforeseen circumstances for which there exists no clear guidance. There also will be differences in interpretation of even the clearest guidelines, particularly when classified or otherwise sensitive information is involved and when agencies have conflicting perceptions of the risks of sharing. The information sharing environment, therefore, must include a systematic, workable, efficient process through which to resolve these disputes. The dispute resolution process can provide practical support to advancing the overarching goal of responsible information sharing.

4. A comprehensive authorized use standard would incorporate a dynamic permissioning process into that standard. That is, if a user seeking classified information cannot make a strong initial case showing that the information is needed for investigation, analysis, or some other important

---

[10] Program Manager, Information Sharing Environment, "Feasibility Report: Report for the Congress of the United States," March 2008, p. 14.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000080 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.048

purpose, a process for developing more information from less sensitive sources should commence. As more is known about need for information and the risks of failing to share, potential users could return to the dispute resolution process with more information and receive new reviews quickly.

If authorized use procedures such as these had been in place, PFC Manning would have had access to Department of Defense information directly focused on the specific issue he was working on as a military intelligence analyst in Iraq. Manning also would have had access to information relevant to his work produced by other departments in the government. However, Manning would not have had access to the 1.6 gigabytes of data that contained sensitive reporting across the spectrum of US government activities. Authorized use significantly reduces the amount of damage any one individual can do. Thus an authorized use standard should be a critical element of any information sharing system as a tool for mitigating the risks of information sharing.

Moreover, authorized use offers multiple operational benefits. It has the potential to reduce uncoordinated action by different agencies and to substantially decrease the level of noise in the system by targeting those who have and need access to information. It facilitates trust, as users must state their purpose for accessing the information as well as how they plan to use it. And when combined with information discoverability, as discussed below, authorized use is a means to identify others who have an interest in the same person or topic so that an interaction and exchange might begin.

Immutable Audit[11]

Transmitting agencies should be required to keep an immutable, auditable record of each dissemination of information for which an articulation of authorized use was made. Maintaining tamper-resistant logs of user activity in the Information Sharing Environment increases security, builds trust among users, measures compliance with relevant policies and guidelines, and improves both transparency and the ability of stakeholders outside of the system to perform appropriate oversight. Such auditing is helpful for securing information from insider compromise and for protecting civil liberties.

Working under an authorized use standard, if audits were to find that an asserted use is not actually within the assigned mission of the receiving unit or individual, or if periodic assessments determine that information is not being used for an authorized use (or not being used at all), then managers and policymakers have an objective basis for reassessing and perhaps terminating the sharing, thus minimizing the risk of information loss, misuse or abuse.

Real-time audits also would play a role in helping identify unauthorized access and, if the allegations against PFC Manning are true, would have triggered immediate technological and human responses, preventing him from downloading more information and alerting counter-intelligence authorities.

---

[11] More information about Markle's previous work on immutable audit is available at www.markle.org/sites/default/files/ustf_IAL_020906.pdf.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000081 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.049

Auditing these immutable logs would have the added benefit of creating new intelligence and knowledge for analysts, policymakers, and others, as well as facilitating dispute resolution by creating real-time, electronically-accessible records that automated software can use to identify common questions presented by different analysts.

Implementation

Making information sharing more secure should go hand-in-hand with making the information sharing environment more effective and trusted by both those working to protect us and by the American people. Critical additional elements of an effective information sharing system that require further development include deepening government-wide policies for sharing information about US persons, discoverability of information, metrics to assess progress, and sustained leadership to bring change across the entirety of government.

US Persons Policies[12]

Government-wide privacy and civil liberties policies for sharing information about US persons must be deepened to match increased technological capabilities to collect, store, and analyze data. Director of National Intelligence Clapper noted in a recent Threat Assessment delivered to the House Permanent Select Committee on Intelligence that homegrown extremists now "play a disproportionately large role in the threat to US interests because of their understanding of the US Homeland, connections to compatriots back in the United States, and relatively easy access to the Homeland and potentially to US facilities overseas."[13] Furthermore, it is becoming increasingly difficult to distinguish between foreign collection and US Persons collection because of the transnational nature of terror groups.

Progress has been made in understanding how information about US Persons can be collected and used, and the predicates for such use. However, much more work is needed on government-wide policies regarding collecting data on US Persons. Inconsistent interpretation of US Persons law across the government can result in government personnel not taking full advantage of lawful activities because individuals are not certain how the law applies to specific cases. This has led to risk aversion when collecting and sharing critical information about US Persons that might stop terrorist attacks.

Consistent and transparent policies regarding the use of US Persons data are necessary to both empower the participants in the information sharing environment and assure the American people that their civil

---

[12] More information about Markle's previous work on US Persons policy and other privacy issues is available at http://www.markle.org/sites/default/files/20090717_nstfprivacy.pdf.

[13] Prepared Testimony of James R. Clapper, Director of National Intelligence, before the House Permanent Select Committee on Intelligence, 112th Cong., 1st Sess., 10 February 2011, available at http://www.dni.gov/testimonies/20110210_testimony_clapper.pdf (last visited 1 March 2011).

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000082 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.050

liberties are being protected by the government. Such policies could help prevent the next intelligence failure based on an agency claiming it was not authorized to use information on US Persons.

Discoverability[14]

Like a library card catalog that offers information on books but not the books themselves, discoverability offers users the ability to discover data without gaining access to the entire record unless or until it is authorized. All data within a distributed information sharing environment should be made "discoverable." Through the use of indexes (the cyber equivalent of library card catalogs), users are able to discover data that exists elsewhere, returning pointers to data holders and documents. Requiring agencies to tag their data is a critical first step toward discoverability.

In addition, systems should be put in place so that data can find data. Data finding data links an arriving piece of information to existing information such that insight will emerge automatically when analyst attention is warranted. This process can be automated using existing technology so that notifications can be sent to users when new data reveals a connection that may warrant attention. Such notifications would help focus the finite investigative resources of the US government (e.g., by highlighting new information for select individuals who have previously expressed interest in a topic, much like when Amazon.com recommends new books based on a user's order history). When data finds data, such a distributed network can empower people at the edges of the system by enabling human collaboration to be directed to the most pressing issues. However, individuals would not have access to the content without further action.

Commercially available technology exists to enable discoverability, and this technology has proven effective on a large scale in numerous private sector applications. In fact, commercial off-the-shelf technology built specifically to enable the government to achieve goals such as discoverability, selective revelation, real-time and immutable auditing, and enforcing an authorized use standard, is in use already at a number of government departments and agencies.

Metrics

Metrics are a critical management tool that can catalyze the further work that is needed to improve government's ability to understand threats and also manage information access. By the 10th anniversary of 9/11, a baseline set of metrics needs to be established so that progress toward discoverability and other key information sharing goals can be quantitatively measured against that baseline. Scores on these metrics should be taken into account in budgetary decisions immediately. Such metrics can help overcome bureaucratic resistance to change by creating significant consequences for inaction.

---

[14] More information about Markle's previous work on discoverability is available at www.markle.org/sites/default/files/20090825_discoverability.pdf.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000083 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.051

Sustained Leadership

As we have emphasized in all the Markle Task Force reports, Presidential leadership continues to be critical for building an effective and reliable information sharing environment. Because information must be shared between and among all levels of government and the private sector, leadership on information sharing must come from the White House, not from a person limited to the intelligence community such as the DNI.

To this end, we have long advocated that the PM-ISE be on the National Security Council staff or be at the Office of Management and Budget. Empowering the PM-ISE at this level increases the potential for the government to stop the next terrorist attack *and* the next unauthorized disclosure.

Conclusion

The 9/11 Commission identified ten lost operational opportunities to derail the 9/11 attacks—and most involved a failure to share information. Progress on information sharing is the single most important step required to improve the national security of the United States. If there is another massive terrorist attack on the United States, the American people will neither understand nor forgive a failure to have connected the dots.

The lesson we should take away from the unauthorized release of classified information to WikiLeaks, then, is not that we should reduce or stop sharing information. Instead, as we develop the capability to better share information, we need at the same time to develop the policies, processes and organizational culture that control access and use. Only by doing this can we build an Information Sharing Environment that those who are working to protect us will trust and use, and that the American people will trust to protect their privacy and civil liberties.

VerDate Nov 24 2008 13:31 Jan 24, 2012 Jkt 66677 PO 00000 Frm 000084 Fmt 06601 Sfmt 06601 P:\DOCS\66677.TXT SAFFAIRS PsN: PAT

66677.052

Questions for the Record Submitted to
Under Secretary Patrick F. Kennedy
Senator Joseph I. Lieberman (#1)
Senate Committee on Homeland Security and Governmental Affairs
March 10, 2011

Question:

Your testimony references the fact that the State Department has removed its database of diplomatic cables (known as the "Net Centric Diplomacy" database) from DOD's classified SIPRNet network. Although the State Department has other means of disseminating its cables, this database was a valuable resource for many interagency partners. In light of this decision, what is the State Department's plan for ensuring appropriate interagency dissemination of diplomatic cables over the long term? Will the Department consider putting its cables on SIPRNet again after security improvements have been made?

Answer:

The Department of State is maintaining our commitment to fully share our diplomatic reporting relied upon by our interagency partners. The primary means through which we share our diplomatic reporting is by automatic dissemination to over 65 agencies based on profiled requirements that these agencies provide to the Department. Recent events have not changed our commitment to sharing this vital information.

The Net-Centric Diplomacy (NCD) database contains a fraction of the cables disseminated by the Department. The primary content found in NCD are cables marked with the caption "SIPDIS," meaning for SIPRNet Distribution. NCD is still available to cleared personnel on the Joint Worldwide Intelligence Communications System, despite its suspended access on SIPRNet.

The Department will continue with our legacy method of dissemination and is exploring options to make cable metadata available to the interagency community on SIPRNet. Any decision by the Department to resume the dissemination of cables or information about cables on SIPRNet will depend on the extent of security improvements that are made.

66677.053

Questions for the Record Submitted to
Under Secretary Patrick F. Kennedy
Senator Joseph I. Lieberman (#2)
Senate Committee on Homeland Security and Governmental Affairs
March 10, 2011

Question:

Section 4.1(i) of Executive Order 13526 modifies the so-called "third agency rule" to allow that "classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order."

Has the State Department implemented this provision of EO 13526? What changes, if any, has State made to its policies and procedures (including marking instructions) in order to implement this provision?

Answer:

When this change to the "third agency rule" went into effect last June, policies and procedures governing the use of markings/captions were already in place at the State Department. Additional guidance was given to all personnel to consider whether special restrictive handling and distribution markings should be added when drafting telegrams, e-mails, and other communications. Instruction on classification management and markings, including restrictive distribution and handling captions, has been included in a computer training course that is to be mandatory for all personnel with authority to classify information.

66677.054

Questions for the Record Submitted to
Under Secretary Patrick F. Kennedy
Senator Scott P. Brown (#1)
Senate Committee on Homeland Security and Governmental Affairs
March 10, 2011

Question:

The Net Centric Diplomacy Database, the database which held the diplomatic cables released by Wiki-leaks, seems to have been made accessible on SIPRNet without regard for the sheer number of users with access to that network, nor a true understanding of the contents of the database. Is that a fair assessment? Why or why not?

Answer:

With regard to this assessment of the Net-Centric Diplomacy (NCD) database, the number of users and the nature of our diplomatic reporting via cable were considerations when allowing NCD access via the Secret Internet Protocol Router Network (SIPRNet). NCD was created in a post-9/11 need-to-share environment. The creation of NCD was a collaborative, interagency effort funded and supported by the Department of Defense and the Office of the Director of National Intelligence.

NCD leveraged web-based technology to provide more immediate access to national security information (classified and unclassified) by cleared professionals working around the world on SIPRNet.

Regarding NCD's content, State cables with the "SIPDIS" caption, meaning for SIPRNet distribution, are automatically stored in NCD when they are disseminated by the Department. The SIPDIS caption denotes that information in a cable is intended for the widest possible audience with an appropriate need-to-know. NCD was made available on SIPRNet because it is a network with a large user community of cleared personnel, so the number of users had been considered during NCD's inception. Guidance on both content of telegrams with the "SIPDIS" caption, and the reach of SIPRNet were provided telegram drafters and approvers.

66677.055

Questions for the Record Submitted to
Under Secretary Patrick F. Kennedy
Senator Scott P. Brown (#2)
Senate Committee on Homeland Security and Governmental Affairs
March 10, 2011

Question:

In a Washington Post article from December, you said that the Department was not equipped to "perform independent scrutiny over the hundreds of thousands of users authorized by the Pentagon to use the database."

a. Were these concerns expressed before the database was developed and put on SIPRnet or only in retrospect?

b. If before, who were they expressed to and what was the resulting feedback?

Answer:

My comment in the Washington Post article was an observation about information sharing and trust between and among agencies—it reflects the Department's belief that once an agency's information is provided or made available to another agency, it is the responsibility of the receiving agency to securely disseminate that information within that organization according to its needs and the safeguarding requirements of Executive Order 13526.

Additionally, we share certain categories of classified information, with agencies based on various agreements and understandings regarding how information will be accessed, protected, and used. It is the receiving agency's responsibility to secure and make accessible the received information based on agreed upon terms. Recipient agencies are expected to maintain adequate security for their own systems and networks.

66677.056

Questions for the Record Submitted to
Under Secretary Patrick F. Kennedy
Senator Scott P. Brown (#3)
Senate Committee on Homeland Security and Governmental Affairs
March 10, 2011

Question:

The Wiki-leaks release of State Department cables, for instance, didn't contain any Top Secret documents, just those at the Secret-level and below. After a situation like this and the release of such a large amount of data, there are concerns that agencies and the current Administration might be pushed to elevate the classification of documents unnecessarily. This is not necessarily a transparency issue, so much as complicating efforts for sharing information between agencies. There are concerns of a tendency to elevate the classification of documents to further restrict access, for instance, to keep them out of SIPRNet. What are you doing to prevent this from occurring at State?

Answer:

The State Department maintains our commitment to fully share our diplomatic reporting on which our interagency partners rely. Guidance has been provided to domestic offices and our diplomatic posts regarding the appropriate use of distribution and control captions and markings on documents when sensitivity and other considerations require. The Department's online training course, which is mandated by Executive Order 13526, includes training on the proper level of classification as well as classification management and markings, including distribution and handling captions.

CHARRTS No.: SHSGAC-01-001
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson
Senator: Senator Ensign
Question: #1

Senate Bill 315: Securing Human Intelligence and Enforcing Lawful Dissemination Act

Question. I have introduced legislation in the form of Senate Bill 315, "Securing Human Intelligence and Enforcing Lawful Dissemination Act," that would include as prohibited classified information, that which would benefit a transnational threat, and that which relates to the human intelligence activities of the United States or any foreign government or concerns the identity of a classified source or informant of an element of the U.S. intelligence community (IC).- What is the Department of Defense's and the IC's view of this legislation?- What recommendations would you make to improve this legislation?

Answer. DoD would defer to the Department of Justice on the issue of possible gaps in legal authorities to prosecute disclosures of classified information.

66677.058

CHARRTS No.: SHSGAC-01-002
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson
Senator: Senator Ensign
Question: #2

Afghan Informants Potentially Identified by WikiLeaks

Question. In an article published July 28, 2010, The Times reported that the documents published by WikiLeaks on its website put at risk hundreds of Afghans as the files identified informants working with NATO forces. The Times, after just two hours of searching the documents, located the names of dozens of Afghans identified as having provided information to the United States. These people were identified by their villages and in some instances, by their fathers' names. Further, after WikiLeaks published 400,000 classified documents concerning U.S. efforts to promote democracy in Iraq, Pentagon spokesman Geoffrey Morrell stated that the Department of Defense rushed to notify approximately 300 Iraqis out of concern for their immediate safety. Morrell also expressed DoD concerns that as many as 60,000 Iraqis could be identified in the leaked documents. The Taliban has publicly boasted that it has killed some of these individuals.- Have any individuals in Afghanistan, Iraq or elsewhere been physically harmed because their identity was either revealed or indicated in a document posted by WikiLeaks?- What specific measures have the DoD and IC taken to affirmatively confirm the safety of the individuals mentioned in the leaked documents? Please be as specific and detailed in your answer as possible.- If the United States government has not been able to confirm their safety, what are the reasons for this, and what renewed efforts are being made to confirm their safety? Again, please be as specific as possible and provide justification if renewed efforts are not being made.- Have the Taliban claims been proven or disproven and what intelligence do we have to make such a determination?- Have U.S. or Coalition forces been forced to relocate individuals due to safety concerns stemming from their names being posted by Wikileaks? If so, who are these individuals and where were they relocated?

Answer. [Deleted.]

66677.059

CHARRTS No.: SHSGAC-01-003
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson
Senator: Senator Ensign
Question: #3

WikiLeaks

Question. Should we be concerned that WikiLeaks has access to other sensitive information, such as identities of informants related to organized crime, drug cartels or street gangs, that would also place the lives of human intelligence sources, confidential informants or undercover agents in danger?

Answer. [Deleted.]

66677.080

CHARRTS No.: SHSGAC-01-004
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson
Senator: Senator Ensign
Question: #4

Compromised HUMINT Source Contingency Plans

Question. In the event it is discovered that further human intelligence sources have been identified or compromised, what are the contingency plans of the United States government to deal with this?

Answer. [Deleted.]

66677.061

CHARRTS No.: SHSGAC-01-005
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson
Senator: Senator Ensign
Question: #5

WikiLeaks Redaction of HUMINT Sources

Question. Is there any evidence that U.S. efforts have influenced WikiLeaks and similar other organizations to redact the names of human intelligence sources?

Answer. [Deleted.]

66677.082

CHARRTS No.: SHSGAC-01-006
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson
Senator: Senator Collins
Question: #6

Insider threat

Question. The response to the divulgence of classified cables in the WikiLeaks incident appears to be focused on technology, despite the fact that media outlets have reported extensively on Private Manning's red-flag behavior during his time in the Army. In particular, reports detailed mental health issues, an assault on colleagues, and the fact that superiors had questioned whether he should be sent to the front lines. The case is similar to another Department of Defense (DoD) case this Committee just reviewed -- the tragedy of Fort Hood, and how many in DoD turned a blind eye to obvious signs of Major Hasan's radicalization. As General Keane (ret.) testified at the Committee's recent Fort Hood hearing, DoD can sometimes do this when there is a pressing need to fill particular positions. We have yet to see the results of the Counter-intelligence Executive's review of what happened in this case; however, it appears that obvious personnel and discipline issues should have prompted extra scrutiny of someone working with classified information.

(a) Were there adequate security checks in place to counter the insider threat that Private Manning posed in this case, and does DoD plan to make changes to its system of security checks in light of this incident?

(b) When do you expect the Counter-intelligence Executive to complete its review of this case?

Answer. We have assumed this question refers to the January 2011 Office of Management and Budget letter to all agencies requesting that an initial assessment of security policy and procedure be conducted in anticipation of discussions with the Office of the National Counterintelligence Executive (ONCIX) and the Information Security Oversight Office (ISOO). We have completed our assessments and have also been working with the two organizations to have on site discussions. No dates as yet are confirmed.

66677.083

CHARRTS No.: SHSGAC-01-007
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson, Ms. Takai
Senator: Senator Lieberman
Question: #7

Insider threat

Question. Your testimony describes actions that the Department of Defense is taking to review current security policies, procedures and technologies and prevent future leaks of classified information by trusted insiders. In these reviews, what is the Department doing to anticipate future security threats and vulnerabilities that may arise due to changes in technology?

Answer. The Department of Defense, as a matter of routine process, is always examining how technology is changing in the near, mid and long-term and an essential part of the process is how that technology will help or challenge our security posture. We especially look at how changes or new technology can be attacked or subverted by external actors, as well as insiders, and develop processes and procedures to mitigate that risk.

CHARRTS No.: SHSGAC-01-008
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: Ms. Takai, HON Ferguson
Senator: Senator Lieberman
Question: #8

Monitoring of Classified Networks

Question. What is the Department of Defense doing to improve real-time (or near real-time) monitoring and auditing of its classified networks and systems as a result of the unauthorized Wikileaks downloads and releases?

Answer. The department has long recognized the potential damage from an insider threat or malicious behavior in our expanded information sharing environment. In addition to the Host Based Security Systems (HBSS) and related enhancements identified in my testimony, a USSTRATCOM led gap analysis is being conducted to identify weaknesses in planned or programmed capabilities. The results of this analysis, due late this fiscal year, will be considered in future tool or process improvements. Additionally, the Department has embarked on a continuous monitoring strategy for its networks, consistent with OMB FISMA reporting requirements, which will include near real-time monitoring for secure configurations.

66677.085

CHARRTS No.: SHSGAC-01-009
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: Ms. Takai, HON Ferguson
Senator: Senator Lieberman
Question: #9

Supply Chain Security

Question. Is the Department of Defense reviewing the issue of how security requirements are integrated into the Department's procurement and acquisition processes as part of its broader post-Wikileaks review? If so, what issues are being looked at and what changes have been made or are under consideration?

Answer. Information system security requirements are integrated into the Department's acquisition and procurement processes and validated through DoD's Information Assurance certification and accreditation (C&A) processes. During the Department's review there were no problems identified related to the procurement and acquisition processes, but there were clearly failures in the forward areas in following the C&A process for systems in operation to insure the security status was maintained. This was more a failure of leadership in the deployed element than in the C&A process itself, but there are changes being made to the C&A processes to incorporate more continuous monitoring requirements which will address the problem identified in WikiLeaks. Deployment of the Host Based Security System and its ability to immediately identify and report misconfigured systems, both to local and Department level security operations centers, will also address the issue.

The Department also plans to update the National Industrial Security Program Operating Manual (NISPOM), which establishes national baseline standards for the protection of classified information in industry. In accordance with Subpart 4.4 of the Federal Acquisition Regulation, all contracts requiring access to classified information must include a standard clause which requires the contractor to comply with the protection standards for the protection of classified information specified in the NISPOM. Sec. 201(e) of Executive Order 12829, National Industrial Security Program, requires protection standards for industry to be "consistent" with the standards for Federal Agencies. Therefore, when protection standards for classified information for Federal Agencies are updated, the NISPOM will be similarly revised.

66677.086

CHARRTS No.: SHSGAC-01-010
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson, Ms. Takai
Senator: Senator Lieberman
Question: #10

EO 13526 Classification Guidance

Question. According to a recent article at Secrecy News, the Department of Defense has not yet published updated implementing regulations on classification guidance, as required by Executive Order 13526 < http://www.fas.org/blog/secrecy/2011/02/reform_stymied.html>. Is this report accurate? If it is, is the Department of Defense currently working on updated implementing regulations, and what is its timetable for completing them?

Answer. The article you mention is inaccurate on a number of counts, and Mr. Aftergood did not consult with the DoD office responsible for updating this issuance. He is correct that the policy in DoD 5200.1.R, "Information Security Program," dates from 1997. A new manual, which will update this policy, as well as consolidate several policies into a single, four volume guide for the field, has been in development since 2009.

DoD policy issuance is a very thorough process that coordinates policy across the entire department and includes legal reviews at multiple stages. Each comment or change receives a thorough adjudication which must be accepted by the commenting components. We notified the Information Security Oversight Office (ISOO) that DoD would not be able to reissue the policy in the timeframe allowed; however, ISOO and the National Security Staff denied the DoD request to extend the deadline established in the Executive Order (E.O.) 13526 and its implementing directive.

The good news is that this new DoD manual is in final comment adjudication. It will require DoD components to complete a Fundamental Classification Guidance Review and to take into account all relevant guidance from the new E.O., President's memo, and implementing directive.

In October 2010,we sent formal notification to all DoD components reminding them of their obligation to comply with the E.O. as well as with the President's memo. We also initiated a DoD wide update of classification guidance. As a result, in 2010, the Department went from only 30% currency of its classification guides to over 70%.

To provide additional guidance to DoD components in the interim, the Department established a Defense Information Security Advisory Board (DISAB) with membership from across DoD, which drafted and sent correspondence on the subject of the Fundamental Classification Guidance Review.

ISOO and Mr. Aftergood may not understand the enormity of such an undertaking for DoD. DoD has more classification guidance than any other agency or Department by several orders of magnitude. The limited resources available for conducting such a review are already over-tasked by several new initiatives and activities resulting from the EO as well as other circumstances such as the WikiLeaks disclosure. Regardless, the Department has made solid strides forward in implementing the national policy contrary to Mr. Aftergood's assertions.

66677.067

CHARRTS No.: SHSGAC-01-011
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson, Ms. Takai
Senator: Senator Lieberman
Question: #11

EO 13526 Section 4.1(i)

Question. Section 4.1(i) of Executive Order 13526 modifies the so-called "third agency rule" to allow that "classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order."Has the Department of Defense implemented this provision of EO 13526? What changes, if any, has DOD made to its policies and procedures (including marking instructions) in order to implement this provision?

Answer. The Department is in the final stages of coordinating updated information security policy that implements all of the provisions of E.O. 13526. This updated information security policy will include a provision for marking documents so that the recipient can identify the information that would require originator approval for release to a third party. This provision will be contained in the marking volume of the revised Information Security Program policy (DoDM 5200.01). The revised policy also explicitly includes the modified "third agency" rule as it relates to dissemination of classified information outside of the Department of Defense.

66677.088

CHARRTS No.: SHSGAC-01-012
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: Ms. Takai, HON Ferguson
Senator: Senator Brown
Question: #12

Deploying New Tools and Technologies

Question. In testimony and supporting materials presented for the hearing, new tools and technologies being implemented at federal agencies were mentioned several times. Some are being used to better assist with active monitoring of classified user activities. Others are enhancing the capabilities of intelligence analysts to sift through large amounts of data. As a result of both the speed in which new technologies become available and the pressure on agencies to improve their analysis and info-sharing capabilities, there are concerns that new systems are being deployed without the proper internal controls and procedures being put in place first.

a. What are your concerns about the pace at which new technology is rolled out and the quality of internal security controls and policy put in place before their deployment?

Answer. Although the pace of technology has accelerated, the Department has policy and processes in place, which require a measured risk assessment of internal controls required and applied before information systems are authorized to operate. Additionally, we are constantly researching potential vulnerabilities using internal Department assets and capitalizing on our close partnership with prominent information security product vendors to identify and resolve issues

b. What steps has DoD taken to address this issue?

Answer: Our 8500 series of departmental directives and instructions are designed for just that purpose. The Defense Information Assurance Certification and Approval Process contained in DoDI 8510.1 is the primary policy insuring information system security controls are adequate. That instruction is being updated and aligned with the recent NIST SP 800-53 issued risk management framework to ensure a more balanced risk decision is made prior to allowing information system operation.

c. How often is this an issue with new systems that are added to SIPRnet and other classified networks?

Answer: The information systems employed on the classified networks undergo the same authorization to operate process described above. Any newly identified vulnerability is managed and mitigated in the same manner as for our unclassified networks.

d. Your joint testimony with Mr. Ferguson talks about integrating new "role-based" access

66677.089

controls to sensitive systems and stronger audit capabilities. It is obvious that these types of controls were not in place or properly utilized before the Wiki-leaks release. What was preventing these tools and procedures from being implemented in the first place? Lack of knowledge? Lack of senior-management leadership?

Answer: "Role based" access controls require strong user identity that will be enabled with our deployment of Public Key Infrastructure on the SIPRNet, which began this year and will be completed in 2012. However, it is a complex problem to determine the "catalogue" of roles that apply across the USG and the attributes which are associated with those roles, identify (or create) authoritative sources for the attributes, and determine what information would be made available to a specific role. While we are moving forward to get some of the necessary technology in place to provide role-based access (the identity token, application design that can sort information by role), it has been a "knowledge" problem to identify the roles themselves and then decide what information gets shared with a particular role. Role-based or attribute-based access control, if not implemented with great care, brings significant risk of causing intelligence – and therefore operational – failure. The Department is revising its approach to governance of intelligence enterprise IT and strengthening our collaborative approach to management of IT-related intelligence activities among OUSD(I), the DoD CIO, and the IC CIO. Our goal is to improve data and information control capabilities, while retaining the information sharing capabilities we have implemented.

CHARRTS No.: SHSGAC-01-013
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson, Ms. Takai
Senator: Senator Brown
Question: #13

Maintaining Security Procedure Compliance

Question. Establishing more robust security procedures and protocols is one thing, but maintaining visibility over continued compliance to these policies is another concern. Articles on Private Manning's exploits talk about how he was asked how the data containing the classified data was insecure. He replied that after consistently working 14-hour days, people "stopped caring after three weeks." You can write a great manual on security procedures, but following up to make sure people are consistently following these procedures is equally, if not more important.

a. What is DoD doing to ensure continual compliance to rules and regulations regarding access and working in classified networks?

Answer: We have established the first formal security oversight and assessment program to determine levels of compliance and recommend policy and procedural changes for implementation within the components. In addition, USSTRATCOM /USCYBERCOM is monitoring use of the SIPRNet and now has a mechanism for reporting certain anomalous behaviors for appropriate remediation. Simply understanding that we have this monitoring capability creates deterrence of willful mischief.

Leadership is critical for ensuring compliance and establishing accountability. Senior leaders across DoD, to include the Secretary of Defense, have formally announced an expectation of individual responsibility and accountability, and DoD is in the process of developing on-line security violation reporting mechanisms so that we have a record of issues to use as the basis for taking actions as appropriate.

b. Are there plans to do anything like a red-team or unannounced inspections, something to that effect?

Answer: At present, no resources have been identified to conduct such inspections DoD wide. However, several DoD components have reinvigorated random physical inspections of personnel. Additionally, the interagency, through the National Security Staff, is considering national level options for oversight inspections. However, national information security policy requires self-inspection, so we are in the process of providing more detailed guidance to the Components for the conduct of these self-inspections, consistent with Information Security Oversight Office guidance.

c. How are we monitoring personnel in the field such as in Afghanistan?

66677.071

Answer: As discussed earlier, USSTRATCOM/USCYBERCOM is monitoring data transfer activity on the SIPRNet to identify anomalous behavior. DoD is examining options for more robust monitoring capability as well as implementing Public Key Infrastructure on SIPRNet to understand specific individual use of the system.

d. What is DoD doing to eliminate the type of apathetic attitude that can occur during long deployments as described above?

Answer: Leadership and accountability are critical to ensure against complacency and apathy. Training and education are also key elements in combating this inertia. In this case, leaders were held accountable and all personnel were reminded of their individual responsibilities. We are also in the process of mandating security training for all personnel prior to deployment and re-emphasizing mandatory annual training in security for all DoD personnel.

CHARRTS No.: SHSGAC-01-014
Senate Committee on Governmental Affairs
Hearing Date: March 10, 2011
Subject: Information Sharing
Witness: HON Ferguson, Ms. Takai
Senator: Senator Brown
Question: #14

Over-classification

Question. The Wiki-leaks release of State Department cables, for instance, didn't contain any Top Secret documents, just those at the Secret-level and below. After a situation like this and the release of such a large amount of data, there are concerns that agencies and the current Administration might be pushed to elevate the classification of documents unnecessarily. This is not necessarily transparency issue, so much as complicating efforts for sharing information between agencies. There are concerns of a tendency to elevate the classification of documents to further restrict access, for instance, to keep them out of SIPRnet. What are you doing to prevent this from occurring at DoD?

Answer. DoD has a culture of sharing that is well established, particularly in a warfighting environment. We do have concerns that the disclosures will have a chilling effect on sharing - perhaps by over-classification - but we are not aware of any evidence that this has occurred to date. Agencies are required to classify information based on security classification guidance established by Original Classification Authorities (OCAs). OSD security staff is working with all of the DoD components to establish better and more up to date classification guidance to ensure that we are applying the appropriate standards to classification decisions.

66677.073

Post-Hearing Questions for the Record
Submitted to Corin R. Stone
From Senator Joseph I. Lieberman

"Information Sharing in the Era of Wikileaks: Balancing Security and Collaboration"
March 10, 2011

1. **Your testimony describes actions that the Intelligence Community is taking to review current security policies, procedures and technologies and prevent future leaks of classified information by trusted insiders. In these reviews, what is the IC doing to anticipate future security threats and vulnerabilities that may arise due to changes in technology?**

   The ever-increasing volume of information available to the IC in the Internet age will continue to require technology solutions to effectively manage the attendant risk. Positive identity management is the first step – knowing exactly who is accessing our networks rather than allowing people to access systems anonymously. We will improve our ability to individually track users through enforcement of strong user authentication on classified networks, ensure responsible controls on removable media, and provide strong website authentication for classified fabrics – all to provide greater control over access to classified information. NCIX will also implement a comprehensive Insider Threat Program across government to ensure security and counterintelligence controls and responses meet the dynamic threat and risks of changing technology and human tactics. Additional security controls consistent with NIST SP 800-53 will be employed to anticipate future security threats and address the risks of changing technology.

2. **Your testimony discusses the importance of "auditing and monitoring" as a key element of efforts to improve the security of classified information. What kind of auditing and monitoring is currently in place in major intelligence community systems? Is the IC upgrading its auditing and monitoring capabilities as a result of Wikileaks, and if so, how?**

   There are differing capability levels of audit and monitoring tools currently in use across the IC. Intrusion detection systems (e.g., firewalls, anti-virus software) protect IC networks from external hacker threats. Recording authorized user logons to IC systems that process classified information is also standard practice. The FBI and CIA have robust insider threat programs in place for tracking the specific information accessed by users of their systems and detecting, to varying degrees, suspicious user behavior (e.g., excessive file accesses or data downloads) and alerting security personnel to take action. Several agencies (e.g., NGA, NSA, NRO) are maturing their audit and insider threat capabilities, while others still lag behind. The WikiLeaks disclosures highlighted the need to "raise the bar" in terms of these capabilities. The IC is harmonizing its phased implementation plan for upgrading audit and monitoring capabilities in concert with the White House-led Interagency Policy Committee responding to WikiLeaks.

Post-Hearing Questions for the Record
Submitted to Corin R. Stone
From Senator Scott P. Brown

"Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration"
March 10, 2011

1. **A Washington Post article from December 2010 attributes the push to add the State Department's Net Centric Diplomacy Database to SIPRnet as an effort by former DNI John Negroponte. Prior to new databases or information being added to SIPRnet or other classified networks, what does ODNI do to ensure that a quality security review has been conducted and proper security controls are in place beforehand?**

   The Washington Post article from December 2010 is in error; State Department's Net Centric Diplomacy Database (NCD) launched on SIPRnet in 2004, preceding stand up of the ODNI. The Information Security Risk Management Committee (ISRMC) oversees the information security risk for Intelligence Community (IC) enterprise systems. Specifically, the ISRMC provides advice and recommendations to the IC Chief Information Officer (CIO) and IC CIO Council on IC enterprise information security risk management activities. Risk-based decisions are made prior to the deployment of systems in operational environments, and reviewed periodically to ensure currency and relevance to the evolving threat landscape. Pre-requisites for a risk decision include selection of security controls based on the impact of a system to IC missions and proof of a thorough security review and its associated findings.

2. **The Wiki-leaks release of State Department cables, for instance, didn't contain any Top Secret documents, just those at the Secret-level and below. After a situation like this and the release of such a large amount of data, there are concerns that agencies and the current Administration might be pushed to elevate the classification of documents unnecessarily. This is not necessarily transparency issue, so much as complicating efforts for sharing information between agencies. There are concerns of a tendency to elevate the classification of documents to further restrict access, for instance, to keep them out of SIPRnet.**

   a. **What are your concerns regarding over-classification as a result of the Wiki-leaks case?**

   Over-classification concerns are largely addressed by IC policy and security classification guidance. Moreover, EO 13526 and recent ISOO guidance concerning Fundamental Classification Guidance Reviews require all agencies with original classification authority (OCA) to review their classification guidance to ensure protection requirements are current and classification guides updated, as necessary. Progress reports must be submitted to ISOO in July 2011, January 2012, and a final report submitted in June 2012.

   b. **What kind of guidance is ODNI providing to reduce this tendency among agencies?**

   The tendency for over-classification is best mitigated through policy and standardized procedures, training and oversight. ODNI has drafted IC guidance for development of formal and informal classification marking challenge procedures. This guidance, being sent to all IC element heads and senior agency officials, requires IC elements to establish procedures to encourage the workforce to submit marking challenges for information they believe is either over or under classified. In addition, the ODNI has drafted guidance reminding IC agencies of their obligation to perform fundamental classification guidance reviews under EO 13526. The ODNI leadership strongly endorses the Information Security Oversight Office's direction to ensure agency/element reviews are thorough, comprehensive and complete regarding classification guidance they issue, and include a requirement for updating classification guides as needed. IC Directive 208 "Write for Maximum Utility" encourages intelligence products to be written at the collateral level and annotated where higher classification versions are available to those who are appropriately cleared and require them. ICD 501 "Discovery and Dissemination or Retrieval of Information within the Intelligence Community" provides guidance for making the existence of all intelligence and related information discoverable, allowing a user additional visibility to challenge classification and access, serving as a check and balance on potential over-classification of information.

Post-Hearing Questions for the Record
Submitted to Kshemendra Paul
From Senator Joseph I. Lieberman

"Information Sharing in the Era of Wikileaks: Balancing Security and Collaboration"
March 10, 2011

1. **In your annual report to Congress on the Information Sharing Environment, you provide agency-specific results from the annual ISE Performance Assessment on a number of metrics related to information sharing. Are you considering updating or revising these metrics in any way as a result of the post-Wikileaks reviews?**

   Yes. The 2011 annual report to the Congress on the Information Sharing Environment (ISE) will reflect mission partner progress against major ISE initiatives that are aligned with the 2007 National Strategy for Information Sharing, and other significant accomplishments of the terrorism and homeland security information sharing and access community. It will also signify a transition to reporting against a new national strategy, currently under development and scheduled for release this year, that will update and replace the 2007 strategy. The new strategy will (1) anchor on the whole of government approach from the National Security Strategy, (2) build upon foundational domestic efforts, (3) open the aperature to the totality of terrorism-related information sharing, and (4) refine the process in which ISE agencies are held accountable by monitoring the operation and maintenance, self-reporting, mitigation of risks, and the performance of the ISE through a combination of quantative and qualitative measures. The metrics used to monitor and report progress on the ISE in the future will be aligned to the new strategy. It is anticipated that those metrics will measure both information sharing and information protection activities as required by the Intelligence Reform and Terrorism Prevention Act of 2004.

Post-Hearing Questions for the Record
Submitted to Kshemendra Paul
From Senator Susan M. Collins

"Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration"
March 10, 2011

1. **One of the programs advanced by the Information Sharing Environment (ISE) is the initiative to advance Suspicious Activity Reporting, or "SARs" within fusion centers and throughout the IC. These include reports that the public provides to government. In late February, a young Saudi student in Texas was arrested after SARs were used to provide leads to the FBI and local law enforcement. Can you please explain how the SAR program has been useful to law enforcement, especially in this case, and how it can be improved?**

One only needs to read the headlines to see that the terrorism threat against our homeland is real – the attempted bombing in Times Square, the FBI arrest of Khalid Aldawsari in Texas, the Christmas Day Northwest Airlines bomber, and the attempted bombing in Portland, Oregon. Every day, in the course of their duties, law enforcement officers observe suspicious behaviors and receive such reports from concerned civilians, private security, and other government agencies. Until recently, this information was generally stored at the local precinct and shared only within the agency as part of an incident reporting system.

The 9/11 Commission Report cited this breakdown in information sharing as one of the reasons why the terrorists were able to carry out their attack, and a recommendation was made to create an environment where law enforcement officers at all levels can share this necessary information.

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), led by the Department of Justice, Bureau of Justice Assistance, has taken the processes that law enforcement agencies have used for years, and established a unified, standards based approach for all levels of government to gather, document, process, analyze, and share information about behavior-based suspicious activities that potentially have a nexus to terrorism while rigorously protecting privacy, civil rights, and civil liberties of all Americans.

66677.078

2. **The Government Accountability Office (GAO) has continued to list terrorism-related information sharing on their biannual "high-risk" list – that is the list of programs that are in danger of waste, fraud, abuse, mismanagement or in need of broad reform. Please provide a specific timeline for getting the ISE off the GAO high-risk list.**

Since 2005, terrorism-related information sharing has been included on the high-risk list – a status which the Program Manager, Information Sharing Environment has agreed with. Although great progress has been made in recent years in analysis of key information and strengthening the sharing of terrorism-related information among Federal, State, local, and other mission partners, additional reform is still needed. The Program Manager, in collaboration with ISE mission partners, will continue to drive reform through the institution of clear, measurable direction in guidance, governance, budget, and performance management with the goal of eliminating redundancies, identifying reuse options, and consolidating similar projects across organizational boundaries. As we work to accelerate the delivery of the ISE, we remain faithful stewards of the taxpayer investment and to ensuring we are truly effective in sharing terrorism-related information to protect the homeland.