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.

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.

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.

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.

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.

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.]

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.]

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.]

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.]

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.

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.

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.

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.

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.

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

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?

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.

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.

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.

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