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

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

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.

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.

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.

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

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

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.