STATEMENT BY

MR. GARY GUISSANIE

ACTING DEPUTY ASSISTANT SECRETARY OF DEFENSE

FOR IDENTITY AND INFORMATION ASSURANCE

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITTEE ON

GOVERNMENT MANAGEMENT, ORGANIZATION AND PROCUREMENT

2154 RAYBURN HOUSE OFFICE BUILDING
MARCH 24, 2010
2:00 P.M.

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT
ORGANIZATION AND PROCUREMENT

Good afternoon, Chairwoman Watson, Congressman Bilbray, and Members of the Government Management, Organization and Procurement Subcommittee. I am Gary "Gus" Guissanie representing the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (CIO). I want to thank you for the opportunity to appear before the Subcommittee to discuss issues related to government wide information security, the Department's efforts to comply with existing FISMA mandates, and initiatives to enhance the nation's cybersecurity[1] through FISMA reform as we go forward.

To paraphrase the Secretary's February 2, 2010, House Armed Services Committee testimony, our military forces depend on digital communications and the satellites and data networks that support them. We face adversaries from individual hackers to nation-states that may seek, without attribution, to damage our command and control operations, intelligence, surveillance, reconnaissance, or precision strike capabilities. With relatively accessible technology and minimal investment, our adversaries operating in cyberspace may, without attribution, damage our command and control operations; intelligence, surveillance, reconnaissance or precision strike capabilities.

[1] The U.S. Government currently defines *cybersecurity* as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation." (NSPD 54/HSPD 23).

Cybersecurity is and has been a critical priority for the Department of Defense (DoD). With information and information technology (IT) assets globally distributed and connected to our partners who actively participate in DoD missions, we know that we cannot execute operations without a robust, assured enterprise network.

This enterprise network approach, coupled with skilled users, defenders, and first-responders working collaboratively with our diverse domestic and international government, intelligence, and civilian partners, including the Defense Industrial Base, will enable us to more readily identify and respond to a cyber attack – and fulfill our missions.

As has been discussed previously before this Subcommittee, the DoD cybersecurity program is aimed at ensuring the following vision:

- DoD missions and operations continue under any cyber situation or condition.
- The cyber components of DoD weapons systems and other defense platforms perform as expected.
- The Department has ready access to its information, including command and control systems, and its adversaries do not.
- The Defense information environment securely and seamlessly extends to mission partners.

Within the Department's overall cybersecurity strategy, a key goal is to "anticipate and prevent successful attacks on data and networks," which closely aligns with the issues being discussed in the community regarding how to better implement cybersecurity measures to defend against increasing cyber threats and vulnerabilities. In concert with the Administration's government-wide information security objectives, we support the focus on continuous monitoring and on the use of real-world penetration testing to maintain a robust security posture. We also consider DoD policies of stringent security testing prior to authorization of systems operation to be a critical element of information assurance. Today, we are progressing toward an enterprise information environment that can dynamically and automatically configure itself to counter threats and facilitate our missions.

FISMA Legislation

The Department has found FISMA in its current form to have significant strengths in improving cybersecurity and would point out that any deficiencies in implementations are not, in and of themselves, sufficient justifications for reform.

One construct that the Department believes is valuable in the current statute that should be retained is the current organizational structure and relationship between the Agency Chief Information Security Officer (CISO) and the Agency CIO. A CISO cannot function effectively if separated organizationally from the CIO and from the operational activity being protected.

DoD Information Assurance Efforts

I will now address Department initiatives to secure our systems within the framework of current FISMA legislation:

DoD Implementation of FISMA

The Department is playing a significant role in multiple efforts to improve the implementation of FISMA. One of those efforts is improving performance metrics and in particular metrics which are feasible for large agencies such as the DoD. The Department recommended a number of improvements to the proposed performance metrics, including:

- Identification of metrics, at the appropriate level of detail, that provide useful information to leadership for assessing the security posture of the organization and enterprise.
- Focusing the proposed automated collection of metrics on the most important metrics for security and management oversight. The Department has been working IA metrics at both strategic and operational levels. As we consider which metrics provide valuable leadership decision-making insight, we are working toward a capability to accomplish "risk scoring" in order to prioritize vulnerability remediation. Eventually we intend to include information on actual threat activities, along with vulnerability data, to enable a more active and flexible defense. Initiatives that roll up raw data, for example: counting workstations, servers, and their operating system versions, when averaged into compliance percentages, lose their meaning when out of

the context of their operational environment. This is particularly true across an environment the size of DoD, or the Military Departments, Defense Agencies or other Defense Components. Because of this, we are building metrics to provide a strategic understanding to senior leadership while employing metrics for the operational Commands.

DoD CNCI and Other IA Activities

The Department is actively implementing a series of initiatives in concert with its IA Strategy and support for the Comprehensive National Cybersecurity Initiative (CNCI). While the Department is aggressively enhancing the security of our systems and networks, the cyber threats in an information-centric world are significant and increasing. Conducting counterterrorism operations, global peacekeeping, homeland security and preparing for escalated warfare make it imperative that IA be viewed not as an IT expense, but as a critical enabler of all national security and defense capabilities. As part of the CNCI and our overall IA Program, the Department is supporting a number of important initiatives, including:

- Acquiring and deploying innovative technologies such as the Host Based Security Solution (HBSS) to increase the fundamental end-point security of our cyber enterprise; thus setting the stage for a unified security baseline. This automated solution will improve security management while reducing costs; increasing the networks' survivability and recovery; and allowing for rapid response to threats targeting the Department.

- NIPRNet Hardening: DoD realigned its access control methodology and operations at the Nonclassified Internet Protocol Router Network (NIPRNet) Internet Access Points, moving from a permit all, deny access by exception policy, to blocking unauthorized access to our private information and supporting systems through whitelisting. Whitelist access is now being used to ensure that only our public facing servers are accessible from the Internet, ensuring that our private servers are not accessible. The most immediate result of these efforts has been to reduce our attack surface by 96 percent. With the full implementation of perimeter DMZs, we will be able to isolate/filter malware at the Internet boundary. As an example, with the removal of spam and malware (viruses, etc.), our first customers at the initial email security gateways have had their traffic loads reduced by 90 percent.
- Defense Industrial Base (DIB): Established a pilot cybersecurity program for the Defense Industrial Base to protect unclassified information relevant to Defense-related research, development and procurement. This effort provides the mechanism to exchange relevant threat information in a timely manner, provides intelligence and digital forensic analysis on threats, and expands Government to Industry cooperation while ensuring that industry equities and privacy are protected. To further this effort, an Advanced Notice of Public Rulemaking was recently published on a possible change to the Defense Federal Acquisition Regulation Supplement (DFARS), which will codify implementation of these pilot security capabilities with our industry partners.

- Supply Chain Risk Management (SCRM): DoD is a co-lead with DHS working to develop a multi-pronged approach for managing risks arising from the globalization of the information and communications technology marketplace. DoD issued a Supply Chain Risk Management Policy now being implemented through several pilot efforts, and the Defense Intelligence Agency has established a Threat Analysis Center to provide supply chain threat assessments to the DoD acquisition community. In January of this year, DoD delivered its "Trusted Defense Systems" report to Congress as we implement a comprehensive trusted defense system strategy targeting full operating capability by fiscal year 2016.
- Joined forces with other federal agencies in the CNCI to secure government networks, protect against constant intrusion attempts, and anticipate future threats.
- Developed and updated the DoD Cyber, Identity and Information Assurance (CIIA) Strategic Plan.
- Partnered with the DNI to establish the Unified Cross Domain Management Office (UCDMO) to synchronize and accelerate the availability of all levels of classified/sensitive information and to protect sensitive or controlled unclassified information to include sharing with our closest partners.
- Contributing DoD expertise to address government-wide information security concerns by partnering with other Federal CIO's and CISO's. The Department is supporting this effort through, among other means, the Department of the Navy CIO co-chairing the Federal CIO Council's Information Security and Identity Management Committee (ISIMC).

- Teamed with the Department of Commerce, the Office of the DNI, and the Committee on National Security Systems (CNSS) to produce a unified information security framework for the federal government -- including a consistent process for selecting and specifying safeguards and countermeasures (i.e. security controls) for federal information systems. This group has already revised control sets for federal civilian and NSS in fiscal year 2009 and, in February of this year, issued the innovative process of the Risk Management Framework as a replacement of the security certification and accreditation (C&A) process.
- Developed Department-wide information systems C&A reciprocity procedures that will ensure the rapid and secure fielding of DoD information systems. Reciprocity will allow mutual agreement among participating enterprises to accept each other's security assessments in order to reuse Information System resources and to accept each other's assessed security posture in order to share information.
- Integrating network and cyber operations in conjunction with the United States Strategic Command to increase our ability to defend the DoD systems and networks.
- Accredited 25 Computer Network Defense Service Providers (CNDSPs) or “CERTS” across DoD.
- Partnered with the National Counterintelligence Executive and Insider Threat Advisory Group to foster collaboration on the use of insider threat tools.
- Promulgated policy on effective use of Internet-based capabilities, including social networking services within the DoD.
- Participating in government-wide cloud computing efforts and a working group

addressing NIST controls for cloud computing.

- DoD also provides a Shared Service Center for Federal IA awareness training at no cost to the participating Federal Agencies.
- Continued to expand the scope and quality of cyber training available to the Department's workforce. In addressing heightened concerns over civil liberties and identity theft, this training includes a review of privacy safeguards and responsibilities to protect personally identifiable information.
- Provided the foundation for the Federal Desktop Core Configuration (FDCC) for a government-wide security baseline for the Windows XP and Vista Operating Systems (OS's). We are continuing our leadership role in this initiative through NSA releasing the draft Windows 7 configuration in fiscal year 2010 and ongoing efforts on other OS's.

DoD IA Workforce

The Department places significant focus on our cyber workforce to help defend the systems and networks. While we aim to achieve robust machine-to-machine network defense capabilities, skilled experts will always remain a critical component in our defense against cyber adversaries. From the everyday user to the cyber defender, the DoD workforce needs to be fully trained and qualified, appropriately deployed, and effectively manned to leverage and protect the Department's significant investment in information and communications. Competency in multiple cybersecurity skills is

demonstrated and evaluated throughout the cybersecurity community through the conduct of joint exercises and is an ongoing core priority of the Department.

To this end, the Department is continuing to expand the IA range capability and quality of cyber training available to its workforce. The technical schools of the military services have expanded their information assurance/cybersecurity curricula to meet DoD common baseline training and certification requirements. The Department has also developed IA awareness training to help users and leaders to better understand their roles in defending DoD networks. In addition, the national Centers of Academic Excellence (CAE) in IA Education are producing graduates with the right skills to achieve a world class cyber workforce that includes both defensive and offensive capabilities. Currently, there are 106 CAEs in 37 states, the District of Columbia, and Puerto Rico, and 32 CAE IA Research Centers in 25 states and the District of Columbia.

Summary

In conclusion, the Department has a strong cyber vision, strategy and supporting program. We continue to work toward a resilient and defendable defense-enterprise network for the Department and for the nation, through collaboration with other Federal agencies to resolve security issues impacting government-wide shared services and infrastructures. The ASD(NII)/DoD CIO is managing a diverse portfolio to comply with FISMA while leading the Department toward Net Centric operations and aggressively working to get ahead of the daunting security challenges facing the Department.