Statement Testimony

The Honorable Zachary J. Lemnios
Assistant Secretary of Defense for Research and Engineering

Before the United States Senate Armed Services Committee,
Subcommittee on Emerging Threats and Capabilities

March 20, 2012

Chairwoman Hagan, Ranking Member Portman, members of the subcommittee, thank you for the opportunity to submit this written testimony on the U.S. Department of Defense's (DoD) cybersecurity Research and Development activities.

I am honored to be joined today by Dr. Michael Wertheimer, the Director of Research at the National Security Agency (NSA), Dr. Ken Gabriel, Deputy Director of the Defense Advanced Research Projects Agency (DARPA), and Dr. James Peery, Director of the Information Systems and Analysis Center at the Sandia National Laboratories.

The Department has a comprehensive strategy for cyber operations, as conveyed in the recently published DoD *Strategy for Operating in Cyberspace.*[1] This Strategy recognizes that cyberspace is an operational domain and a critical element to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations. The FY13 President's Budget Request includes a $3.4 billion investment in cyber activities of which $486 million is for Science and Technology (S&T) activities across Department organizations, to include the Department's organizations testifying here today. This level of investment is significant. The President and the Secretary of Defense recognize the critical importance of ensuring the Department has the required capabilities across the full spectrum of operations – capabilities that protect the Department's enterprise and tactical systems against cyber attack; capabilities that ensure these systems will continue to operate effectively despite cyber attacks; and capabilities that ensure our Joint Forces dominate in any cyber warfare campaign waged against us.

Department's Enterprise Systems

While the cybersecurity challenges to the Department's enterprise information technology reflect those of the private sector in scale and scope, its operational challenges are significantly more complex. The Department operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. The Department's enterprise information technology systems rely upon commercial network service providers and include secure enclaves that protect business data and secure operational data. Breaches of these networks have an impact on national security. The cybersecurity threat to the enterprise is evolving on shorter timelines and with much more aggressive threats.[2] By September, 2011, over 70 million cumulative malware threats were identified; augmented by a new class of tailored social engineering threats that target mobile platforms.

As a first step, the Department began implementation of the Host Based Security System (HBSS) in 2007.[3] The HBSS solution is attached to each host (server, desktop, and laptop) in the Department and is managed by local administrators and configured to address known exploit traffic using an Intrusion Prevention System and host firewall.

---

[1] Department of Defense website: Department of Defense Strategy for Operating in Cyberspace, July 2011
[2] McAfee website: McAfee Threats Report: Third Quarter 2011
[3] DISA Host Based Security System website

In early 2011, the Department began an engagement with the industrial base, through the Enduring Security Framework to build a common threat understanding and best practices for the enterprise.[4] Among the first efforts, this work has developed approaches for improving the security and integrity of computer system Basic Input Output System (BIOS) controls. These concepts have been certified by the National Institute of Science and Technology (NIST) and will be available to the Department through the private sector.[5]

Tactical System Vulnerability Systems

The Department's cybersecurity concerns extend beyond enterprise Information Technology, command and control, and network operations. Tactical system complexity and network dependency create new opportunities for cybersecurity attack and disruption of our warfighting platforms. Tactical systems include manned and unmanned platforms, munitions, control systems, where cyber network attack or exploitation could compromise mission effectiveness. "Perimeter" security techniques engendered by information systems security engineering and other cyber defenses lack sufficient defense for tactical systems should a perimeter defense be compromised. This is increasingly problematic as tactical systems grow in complexity and adversaries have more opportunities for exploit through supply chain or inherent tactical system software, hardware and firmware vulnerabilities. A "system" security approach is required for total mission assurance.

The Department has revitalized its Program Protection policy and practice to apply system security principles to the design, development and fielding of tactical systems. Today's systems are built using a combination of COTS and DoD-unique hardware and software. In the past, the DoD was primarily focused on protecting the release of advanced technology contained in systems, but these systems must also be protected from insertion of malicious content through supply chain attack, and the defense of the system against unauthorized access, control, or alteration during operations. The Department is now applying a comprehensive program protection planning approach as systems mature through the acquisition lifecycle; performing vulnerability assessments, embedding system security engineering and supply chain risk management practices and reducing cyber vulnerabilities.[6] [7]

Enterprise and Tactical Systems Cybersecurity Research

The challenge for the Department's research and engineering enterprise is to develop cybersecurity concepts that will enable the Department's enterprise and tactical systems to operate effectively in today's environment, and to lay the foundation for future capabilities against an increasing complex, capable, and ubiquitous cyber operational threat. Given the many cybersecurity attacks against the Department's networks we have seen over the past few years, we must be prepared to respond rapidly. However, we must also take the long view and

---

[4] Parrish, Karen, American Foreign Press Services: Lynn Urges Partnership Against Cyber Threat , Feb. 15, 2011
[5] NIST Tech Beat: Protecting Computers at Start-Up: New NIST Guidelines, Dec. 20, 2011
[6] Department of Defense Instruction 5200.39: Critical Program Information (CPI) Protection Within the Department of Defense, Dec. 28, 2010
[7] Defense Acquisition Guidebook: Acquisition Protection Strategy for Program Managers: Program Protection Plan

seek fundamentally new concepts and capabilities for cybersecurity. There are no silver bullets that will completely eliminate the cyber threat. The Department's cybersecurity research investments are designed to build a strong technical foundation across the public-private enterprise, supported by robust engineering, modeling, simulation and measurement campaigns.

Four areas are under development to support the "DoD Strategy for Operating in Cyberspace"[1] and have been shaped by a joint DoD and IARPA study. This study reported the independent views of technology leaders from across government, industry and academia who were asked to consider the fundamental challenges faced by Department and the technical approaches that are emerging in academia. The Department's research investments are designed to build technical foundations in the following areas:

- **Mission Assurance:** This focus will enable commanders to successfully execute their missions whether in joint or coalition environments, in the cyber domain and while under cyber attack. This capability requires that our DoD commanders be able to assess and control the cyber situation in the context of the overall mission. Research in this area is in the development of tools and techniques that enable efficient modeling of blue, grey, and red behavior (cyber and kinetic) to determine the correct course of action in the cyber domain.

- **Resilient Infrastructure:** Resiliency is the ability to absorb and fight through cyber-attacks to complete the mission. In the event of an attack, while network performance may degrade, it will not fall below a given critical mission derived level. Achieving this performance characteristic involves developing capabilities that lead to recovery and reconstitution of critical functions in milliseconds. The research in this area is focused in two areas: integrated architectures optimized to speed recovery to a known secure state, and novel protocols and algorithms at the component nodes within the architecture to distribute resiliency mechanisms.

- **Agile Operations:** Agility refers to the ability of systems to dynamically reshape their cyber posture as conditions and goals change, both to escape harm and to thwart the adversary. It requires that networks are able to rapidly change attributes and operating conditions including attack surfaces in near real time. The research in this area is focused on enabling high speed responses with respect to healing, network optimization, and protective cyber mechanisms.

- **Foundations of Trust:** Trust is confidence that our systems – the devices, networks, and cyber-dependent functions – perform as expected, and have not been comprised. DoD systems use components that provide mixed trust levels; some components are provided by domestic and foreign commercial sources, and some components are special highly assured secure components. The research objective for this area is to develop capabilities that result in trustworthy systems even though the components individually have varying degrees of trustworthiness. The technical approach is to

create models that characterize the trust of the systems by observation and analysis of system characteristics and behavior.

The research in these thrust areas supports a range of applications including wired networks, mobile networks, cloud computing, tactical information technology, system security engineering, and trusted components for military systems.

Cyber Testing Infrastructure

The Department's cyber testing infrastructure is comprised of approximately 60 facilities and ranges that support a wide array of activities including research, experimentation, developmental test, operational test, and training. Eleven of these ranges support cyber research and development, the balance are used for training and operational test and evaluation.

The Department has embarked on a strategy to extend interoperability, threat models, traffic generation, and user behavior models for these ranges to support rapid development and test of new cybersecurity capabilities. The Department has testing infrastructure improvement programs in four key areas:

- cyber range automation technology that will enable larger scale, faster turnaround, lower costs, and better utilization of scarce test resources and expertise;
- high fidelity, validated emulations of cyberspace as well as realistic mission scenarios, environment, adversary models, and attack vectors;
- standardized data collection tool suites; and
- cyber measurement framework.

We are exploring two options for how best to integrate cyber range capabilities with the Department's existing test and evaluation infrastructure, which currently supports traditional kinetic missions. The first is to aggregate many of the Department's cyber test resources in a single large cyber-kinetic range, with elements of traditional test ranges on-site. The second option is establish a number of smaller test ranges that can both work independently or be networked together and/or to kinetic test ranges, to support national-level tests and exercises. We plan to evaluate this trade space through a series of tests and pilot exercises during this fiscal year.

Coordination and Transition of Cyber Research Investments

Research and development efforts are well-coordinated among the Department's organization and other federal and international organizations. Since taking office, I have personally met with operational and research leaders at NSA, Combatant Commands, Services, and Agencies to coordinate strategic research thrusts and investments, to assess results, and to identify gaps. Recently, the Department established the Cyber Investment Management Board (CIMB), comprised of the Department's policy, acquisition, and technology leaders, to provide strategic

oversight of the Department's cyber investments supporting the enterprise information technology systems and system platforms.

DoD cyber program research is coordinated among Department organizations through the DoD Cyber S&T Working Group. The membership of the Cyber Working Group includes representatives from across DoD's operational organizations, USSTRATCOM, USCYBERCOM, NSA, DISA, the Joint Staff, and S&T organizations - the Service Labs and DoD Federally Funded Research and Development Centers (FFRDCs). The Working Group's primary task is to develop a roadmap of research programs to include programmatic technical goals, milestones, and investment levels for the four cybersecurity research thrust areas.

Interagency coordination takes place through multiple federal working groups, including the Computer Security and Information Assurance Interagency Working Group – sponsored by the Network and Information Technology Research & Development (NITRD) sub-committee. Further coordination with our allies and partners occurs through the North Atlantic Treaty Organization Research and Technology Organization and the Technical Cooperation Program.

Across the Department, our researchers are engaged with industry, academia and other government laboratories to drive innovation in cybersecurity research and to rapidly transition concepts to operational use. Transition occurs through several channels. Some projects will be adopted for use in commercial technology and involve vendor modifications or the launch of new products. We have seen results in incubating new cybersecurity technologies for commercially available products through our Small Business Innovation Research program. Other projects involve technologies that require the development of custom components and are transitioned through the defense industrial base.

While early research is performed under the management of the Service scientific organizations, much of the applied S&T research and development is carried out through Service laboratories. These organizations maintain connections with acquisition program executive offices, and engineering centers. Through these connections, the Service laboratories share results from emerging concepts and outline joint pilot efforts. These technologies will be available to mitigate vulnerabilities identified in program protection analysis and planning activities performed by program staffs.

Cyber Research and Development (R&D) Workforce and Skill Set

I remain concerned that in emerging and very dynamic technical fields, such as cybersecurity, and system security engineering, the Department needs to build a strong workforce and needs access to the highest caliber technical talent in academia and industry. Formal educational programs address basic cyber threats and fundamental mechanisms of security, but not high end cyber threats, foundations of trust, adversarial reasoning, or game changing approaches. The Department's prospects for satisfying its cyber human capital needs remain challenging due to the following:

- Projected shortages of cyber R&D talent driven by the dearth of clearable candidates electing studies in these areas; this is one area we cannot outsource.

- Limited specialization in cyber academic programs; and
- Significant competition by the private sector.

We are taking an active role in transitioning lessons learned from Cyber R&D to academia to improve cyber education. DoD involvement in the development of formal cyber education will provide interested and formally trained cyber graduates with visibility into research opportunities and career opportunities for public service.

We have several programs underway to advance our cyber R&D workforce through Service labs, Agencies, OSD and National initiatives. I would like to highlight several of these:

- **The Comprehensive National Cybersecurity Initiative**[8] has used competitions to attract high school and college students in cybersecurity. These include CyberPatriot National High School Cyber Defense Competition[9], US Cyber Challenge[10], Department of Defense Cyber Crime Center (DC3) Digital Forensics Challenge[11], and National Collegiate Cyber Defense Competition (CCDC)[12].
- **The Centers of Academic Excellence in Information Assurance Education**[13] recognizes schools with programs that integrate research activities into the curriculum. The schools serve as a source for DoD-academic researcher exchanges; of the 146 centers, 42 are focused on cybersecurity research.
- **The DoD Information Assurance Scholarship Program** is a recruitment, retention and academic capacity-building program.[14] Since the inception of the program in 2001, DoD has sponsored over 470 scholars to complete a degree in a cyber- or information assurance-related field of study.
- **Air Force Office of Scientific Research (AFOSR) Multidisciplinary University Research Initiatives (MURI):** MURIs fund consortiums of universities for complex research problems. AFOSR has 6 MURI research teams addressing four cybersecurity topics. In total over 140 graduate students, 19 post docs and 10 undergraduate students are being trained in the field at 29 universities
- **Service Lab R&D Involvement with Academia:** Over the past ten years, the Information Directorate (AFRL/RI) educated top ROTC cadets and civilian college students on the science of information assurance and trained them in cyber warfare. These programs have graduated over 300 cyber warriors.
- **The Naval Postgraduate School (NPS) Cyber Academic Group**[15] includes course work on cyber operations and planning. Semi-annual Cyber Wargame courses are open to all NPS students. A Cyber Battle Lab with classified and unclassified segments supports interdisciplinary education and research spanning student theses and large projects involving government agencies, DoD, industry, and academia.

---

[8] The White House - National Security Council website: The Comprehensive National Cybersecurity Initiative
[9] CyberPatriot - National High School Cyber Defense Competition website
[10] National Board of Information Security Examiners website: U.S. Cyber Challenge
[11] Department of Defense website: DC3 Cyber Crime Challenges
[12] National Collegiate Cyber Defense Competition website
[13] National Security Agency, Central Security Service website: National Centers of Academic Excellence in Information Assurance Education
[14] Department of Defense website: DoD Information Assurance Scholarship Program
[15] Naval Postgraduate School website: Cyber Academic Group

- **National Security Agency's Cyber Defense Exercise (CDE)** was conceived to evaluate the effectiveness of the IA education instilled at the service academies. DoD provides Red Team participants to this exercise annually to evaluate the performance of the cadets in securing a network. The overall CDE goal is to generate interest among students nation-wide to engage in challenging cybersecurity problems. A team of 38 cadets won the 2011 CDE for the Army.

Summary

Soon after coming into office, President Obama identified cybersecurity as one of the most serious economic and national security challenges facing our nation. The Department of Defense faces particular challenges to its enterprise information technology systems and to its tactical systems. The emergence of networked tactical systems and cyber-physical systems has created new opportunities for increased cybersecurity attack and disruption.

In response to these threats, we are building a strong technical foundation across the research and engineering enterprise. The Department of Defense will develop concepts to enable enterprise and tactical systems to operate effectively in today's environment, and to lay the foundation for future capabilities against an increasing complex, capable, and ubiquitous cyber operational threat.