Countering Cyber Threats through Technical Cooperation with the Department of Defense

April 5, 2016

Fiscal Year 2015 Report to Congress

Homeland Security

Message from the Secretary

April 5, 2016

I am pleased to submit the following report, "Countering Cyber Threats through Technical Cooperation with the Department of Defense."

This report was prepared pursuant to language in House Report 113-481 accompanying the *Fiscal Year 2015 Department of Homeland Security Appropriations Act* (P.L. 114-4).

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable John R. Carter
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Lucille Roybal-Allard
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable John Hoeven
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jeanne Shaheen
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Should you have any questions, please contact me at (202) 282-8203 or the Department's Deputy Under Secretary for Management and Chief Financial Officer, Chip Fulghum, at (202) 447-5751.

Sincerely,

Jeh Charles Johnson

Countering Cyber Threats through Technical Cooperation with the Department of Defense

Table of Contents

I. Legislative Language

This report was prepared pursuant to language in House Report 113-481 accompanying the *Fiscal Year 2015 Department of Homeland Security* (DHS) *Appropriations Act* (P.L. 114-4).

House Report 113-481 states:

> The Committee directs the Secretary to report, not later than 120 days after the date of enactment of this Act, on the current level of cooperation between DHS and DoD, or the possible benefits of cooperation, regarding the development of new and innovative software that improves national capabilities to counter cybersecurity threats. The report should also address the possible use of initiatives at the secondary and post-secondary level; identify the available FTE time of existing cyber experts currently employed by, or contracted with, DoD and DHS; and assess opportunities for the recruitment of veterans into such software development programs.

II. Introduction

The DHS vision of the Internet is of a safe, secure, and resilient infrastructure through which the American way of life can thrive. Many Components in DHS contribute to this mission: the Office of the Chief Information Officer (OCIO), the National Protection and Programs Directorate (NPPD), the Science and Technology Directorate (S&T), the United States Coast Guard (USCG), and the United States Secret Service (USSS). All of these individual Components work together with the Department of Defense (DOD) to protect American interests from cybersecurity threats.

As an ongoing, collaborative process, the level of cybersecurity cooperation between DHS Components and DOD continues to grow in depth, breadth, and scope.

III. Countering Cyber Threats through DHS Cooperation with DOD

Management Directorate, through the Office of the Chief Information Officer, cooperation with DOD

OCIO cooperates regularly with DOD through joint participation in the U.S. Federal CIO Council, the Committee on National Security Systems, and the Federal Risk and Authorization Program. Additionally, DHS is in the process of standing up the Joint DHS Cyber Security Operation Center where the DHS Security Operation Center and the USCG Security Operation Center will operate jointly to counter cyber threats on DHS's .gov domain and USCG's .mil domain.

NPPD Cooperation with DOD

NPPD leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. Accomplishing this mission requires leadership, integration, and cooperation in a whole-of-government approach.

The DHS/NPPD Office of Cyber and Infrastructure Analysis and NPPD Office of Cybersecurity & Communications are reviewing options with DOD for cybersecurity Big Data Analytics partnership activities, including taking into account the physical and cyber threat nexus. These efforts are relevant to the U.S. Federal Government, as well as to critical infrastructure.

Current examples of countering cyber threats through interagency cooperation between NPPD, DOD, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) include Enhance Shared Situational Awareness and the Information Sharing Architecture efforts (formerly the Comprehensive National Cybersecurity Initiative Five). The Enhance Shared Situational Awareness initiative is an effort to create, share, and enhance cybersecurity situational awareness by increasing the speed and quality of cyber information sharing among cybersecurity mission partners, thereby enabling Integrated Operational Actions—a series of coordinated activities undertaken by those who have the capability, capacity, and authority. The initiative developed a high-level architecture and identified standards for sharing different types of information that have resulted in the architecture and implementation of the Information Sharing Architecture. The information covered by the Enhance Shared Situational Awareness initiative includes cyber threat indicators, but it is also broader than that. DHS has a new initiative available through the National Cybersecurity and Communications Integration Center called Automated Indicator Sharing. In short, the Enhance Shared Situational

Awareness effort developed the high-level blueprint, and the DHS Automated Indicator Sharing program has implemented a part of that blueprint at the operational level.

The Automated Indicator Sharing program connects participating organizations to the DHS cyber threat indicator data flow, rapidly sharing cyber threat indicators. This capability enhances the ability of DHS, the Federal Government, and its partners to block malicious cyber activity before intrusions occur. The program not only will share DHS-developed indicators, but also will allow participants to share threat indicators that they have observed in their own network defense efforts. From this pooled information, the Automated Indicator Sharing program will help to build a common, shared knowledge of current threats for use in cybersecurity. This important data flow helps to address cyber threats to our public health and safety, national security, and economic security. The program leverages the work of DHS information-sharing collaborations with federal departments and agencies, as well as DHS-led standards for machine-to-machine communication, and lessons learned from existing DHS private-sector, information-sharing programs to build the framework for this capability. The program also is using feedback from participants to strengthen its implementation along the way. This "crawl-walk-run" approach ensures that the system will be optimized for stakeholder value and participation.

DHS also is leading a community effort to accelerate information sharing between network defense and incident response organizations and communities around the world. These efforts have taken the form of two technical specifications to enable secure, real-time, and actionable sharing activities: the Trusted Automated eXchange of Indicator Information and the Structured Threat Information eXpression. By automating the sharing of anonymized actionable indicators in near-real time, Trusted Automated eXchange of Indicator Information/Structured Threat Information eXpression enables improved situational awareness about emerging threats and facilitates detection, prevention, and mitigation of threats without compromising trust and confidentiality, and appropriately addressing privacy and civil liberties concerns. DHS is cooperating with DOD on plans to migrate DOD information-sharing programs such as the Information Assurance/Cybersecurity Baseline program to use the Structured Threat Information eXpression format. In addition, DHS has moved the Structured Threat Information eXpression and Trusted Automated eXchange of Indicator Information specifications to the Organization for the Advancement of Structured Information Standards to ensure that they are globally recognized standards for the representation and exchange of cyber threat intelligence. DHS and DOD will continue to play a key role in the evolution of these specifications, but the work now will occur under the auspices of a truly global community operating under open and transparent rules.

In addition to partnering to protect the U.S. Government, DOD and DHS also work together through the Enhanced Cybersecurity Services program to provide indicators that can help protect U.S.-based public and private-sector organizations. The Enhanced

Cybersecurity Services program (under a different name) originally was established by DOD to protect defense industrial-based companies. In 2013, the program was transferred to DHS, by Executive Order 13636, in order to allow other sectors to participate. DHS continues to work closely with DOD to source timely, actionable indicators. DHS then shares those indicators with commercial companies that have met security requirements and that can provide services that block malicious traffic to customers. DHS also works closely with NSA to update security requirements, implement new service offerings, and respond to requests for information.

Another real-time example of interagency cooperation to counter cyber threats is the NPPD Office of Cybersecurity & Communications partnership with the NSA. DHS is partnering with the NSA-Information Assurance Directorate and Johns Hopkins University/Applied Physics Laboratory to represent the combined initiatives of Integrated Adaptive Cyberspace Defense. This will result in an evolving application of current and emerging capabilities that address how we combine interoperability, connectivity, automation, information, and trust. Integrated Adaptive Cyberspace Defense is an interagency cooperative effort to shift the current approach and challenge the status quo in cybersecurity toward secure integration and automation to enable faster response times and increase community prevention. Integrated Adaptive Cyberspace Defense is inclusive of Enterprise Automated Security Environment, which is a concept focusing on the enterprise portion of Integrated Adaptive Cyberspace Defense. Enterprise Automated Security Environment is another important step toward achieving the end-state of a healthy cyber ecosystem with automated and dynamic cybersecurity and information-sharing capabilities at the enterprise, intra-enterprise, and interenterprise levels. The DHS and NSA/Information Assurance Directorate partnership is helping to evolve cybersecurity for the entire Federal Government, as well as helping to affect all critical enterprise network owners and operators positively. Integrated Adaptive Cyberspace Defense is a community effort, and the Johns Hopkins University/Applied Physics Laboratory is helping to define the strategy, demonstrate the art-of-the-possible to defenders, and influence the cyber marketplace to promote this change in thinking.

The joint initiatives between DHS and NSA will result in a healthy, resilient, and fundamentally more secure cyber ecosystem. The cyber ecosystem features participants and cyber devices that are able to work together in near-real time to anticipate and prevent malicious cyber activity, limit the spread of such activity, minimize consequences of such activity, and recover to a trusted state. The two components of Integrated Adaptive Cyberspace Defense that will build a more secure future cyber ecosystem are Enterprise Automated Security Environment and Trusted Information Sharing.

DHS also has partnered with NSA since 2004 to co-lead the national Centers of Academic Excellence program. Institutions with Centers of Academic Excellence designation include 2-year, 4-year, and research institutions of higher education that have developed robust cybersecurity programs that meet the Nation’s cybersecurity education needs. There are nearly 200 Centers of Academic Excellences in 46 states, the District of Columbia, and Puerto Rico.

NPPD and the Department are committed to building on the relationship with NSA and U.S. Cyber Command (USCYBERCOM). Our goal is to work with NSA and USCYBERCOM to increase the security and resilience of U.S. critical infrastructure by enhancing interagency collaboration, streamlining information flow, and synchronizing operational activities, from steady-state to incident response.

NPPD also has collaborated with NSA and USCYBERCOM to produce a Cyber Action Plan to provide specific, outcome-based cybersecurity goals and objectives for interagency collaboration. The Cyber Action Plan will engender further a community of trust that streamlines the information flow required to synchronize cybersecurity activities effectively. The plan details objectives and associated action items, which are aligned to overarching goals focused on cooperative efforts over a 12–18-month timeframe. Fully acknowledging that national cybersecurity is a team effort that requires a comprehensive, whole-of-government approach for success, this trilateral plan emphasizes collaborative efforts between DHS, NSA, and USCYBERCOM.

DHS currently is engaged in and making progress with its NSA and USCYBERCOM partners on several items outlined in the Cyber Action Plan. DHS will continue to leverage complementary initiatives, plans, engagements with national cyber centers, and other collaborative efforts that collectively drive toward shared cybersecurity.

S&T Cyber Security Division Cooperation with DOD

The DHS S&T Cyber Security Division mission is to contribute to the enhancement of the security and resilience of the Nation’s critical information infrastructure and the Internet by:

1. Developing and delivering new technologies, tools, and techniques to enable DHS and the United States to defend, mitigate, and secure current and future systems, networks, and infrastructure against malicious cyber activity;
2. Conducting and supporting technology transition; and
3. Leading and coordinating research and development among the research and development community, which includes Department customers, other government agencies, the private sector, and international partners.

S&T’s Cyber Security Division is developing next-generation, research and development, cybersecurity technologies, tools, and technical solutions that address emerging threats and necessary security improvements in critical weaknesses. These solutions include identity and data privacy technologies, end-system security, research infrastructure, law enforcement forensic capabilities, Internet measurement and attack modeling, secure protocols, software assurance, and cybersecurity education.

To accomplish this mission, S&T closely collaborates with a wide range of partners across DHS, other departments including DOD, federal agencies, state and municipal administrations and first responders, critical infrastructure sectors, global Internet governance bodies, cybersecurity researchers, universities, national laboratories, and international organizations.

A. Network and System Security

S&T has partnered with the Naval Postgraduate School to develop a high-frequency topology mapping capability that can be used to discover previously unknown structure, evolution, and temporal dynamics of networks. Extensions of this work currently are being transitioned to DOD and will be of interest to the entire Internet measurement community.

S&T has incorporated results from the Defense Advanced Research Projects Agency Scalable Network Monitoring program into the Framework for Auto-generated Signature Technology program to develop automated signature generation from network traffic. This additional capability will be incorporated in an open source tool (e.g., Suricata) that network administrators and investigators can use to monitor network traffic. The automated signature generation raises the baseline for automated response so that analyst time can be focused on higher-priority events.

S&T has incorporated tests from the DOD-funded Nettest project into the Netalyzr project to add significant monitoring for various network events, such as Domain Name System Security and Transport Layer Security. These tests will detect individual network manipulations and debug problems as they occur. The test results from the Netalyzr project are included in the DHS Protected Repository for the Defense of Infrastructure against Cyber Threats data catalog for further research by both DOD and DHS researchers.

S&T has funded the development of Correlation Layers for Information Query Exploration, a tool that automates several network modeling processes and helps analysts to detect and assess potentially malicious events in billions of network transactions each day. The U.S. Air Force will install the Correlation Layers for Information Query Exploration tools to monitor its network health.

S&T funded the development of the Cartographic Capabilities for Critical Cyber Infrastructure at the Center for Applied Internet Data Analysis that provides state-of-the-art, unclassified, cybersecurity-relevant annotated maps of critical Internet resources.

NSA has been using Center for Applied Internet Data Analysis capabilities to provide DHS with related unclassified information.

S&T has funded an Internet Infrastructure Protection program that provides real-time detection of exploitation and malicious implantation of network equipment. The U.S. Air Force requested that S&T work on specific network equipment (the 3750 router) that has been piloted successfully in Air Force systems. The U.S. Navy is funding further work to apply S&T-developed technologies to shipboard supervisory control and data acquisition systems. The collaboration with DOD will benefit defense as well as nondefense Internet Infrastructure Protection on almost any embedded system.

B. Cyber Physical Systems Security

In addition, the Naval Postgraduate School and S&T have partnered on a project to create a methodology and assessment framework that ensures that desired attributes, such as cybersecurity resilience, are supported and single point network failures are avoided. The initial use will be focused on supervisory control and data acquisition systems on U.S. Navy ships and eventually will be used in public and private infrastructure supervisory control and data acquisition systems.

The Federal Aviation Administration (FAA) has established the Next Gen Cyber Security Working Group that brings together the FAA, U.S. Air Force, National Aeronautics and Space Administration, and S&T to “establish a sustainable foundation for multi-agency collaboration on NextGen cybersecurity.” S&T is participating through the affiliated Interagency Core Cyber Team (the research and development subgroup) under the NextGen Cyber Security Working Group. The goal of the research and development partnership is to develop active, timely, and detailed NextGen cybersecurity collaboration with cyber research and development expertise across the federal and academic communities. Benefits of this collaboration will be to strengthen NextGen capabilities, leverage resources, and avoid technology-related surprise with respect to cybersecurity.

The S&T Cyber Physical Security Program is being coordinated with research efforts in the Defense Advanced Research Projects Agency and with operational DOD government vehicle fleets. The work leverages each department’s investments to provide a more comprehensive solution for general cyber physical security problems and to provide actionable guidance for enhancing the security for both military and civilian government vehicles.

C. Cyber Security for Law Enforcement

The DOD Cyber Crime Center and National Media Exploitation Center participate in the S&T Cyber Forensic Working Group, along with USSS, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, U.S. Citizenship and Immigration

Services, FBI, and the NPPD/U.S. Computer Emergency Readiness Team. The Cyber Forensic Working Group identifies requirements and participates in development and eventual prototype testing of cyber forensics tools, such as vehicle forensics kits and open source forensics tool modules to support the Structured Threat Information eXpression and the Cyber Observable Expression specifications.

D. Education and Training

S&T's Computer Security Incident Response Team research project directly supports the NPPD U.S. Computer Emergency Readiness Team and the NPPD National Cybersecurity and Communications Integration Center. Staff from the U.S. Computer Emergency Readiness Team requested that S&T fund this work, and have assisted with technical review of the project since its start in the fall of 2012. One key part of the Computer Security Incident Response Team project was its ability to leverage team experience with the Navy-Marine Corps Internet as part of its core research effort. The Computer Security Incident Response Team project is producing a Computer Security Incident Response Team management handbook addressing how to design, develop, and operate Computer Security Incident Response Teams and organizations as "multi-team systems." This handbook and its specific guidelines and tools will be transitioned to a variety of Computer Security Incident Response Team organizations in the second quarter of FY 2016, to the NPPD/U.S. Computer Emergency Readiness Team and NPPD National Cybersecurity and Communications Integration Center, to other collaborating organizations, and to several DOD Computer Security Incident Response Team organizations.

E. Other S&T Cyber Security Division/DOD Collaboration

S&T has coordinated cyber-related Small Business Innovative Research programs with DOD's Research and Engineering and Defense Advanced Research Projects Agency since 2004 through co-funding programs and collaborative assessment of each other's programs, and by holding a joint annual conference to review progress of Small Business Innovative Research cybersecurity programs. Collaboration results include a Defense Advanced Research Projects Agency co-funded effort to develop a root kit detection technology that was commercialized through Microsoft and deployed across DOD and non-DOD networks, and Endeavor Technology's Malware Analysis Engine that was transitioned to McAfee for commercialization that includes deployment by DOD in its network Host-Based Security System program.

S&T has participated in Program and Technical reviews hosted by the DOD-funded Carnegie Mellon University Software Engineering Institute that have developed into an ongoing conversation between S&T and DOD about directions and priorities of unclassified cybersecurity research and development. The ongoing conversations will lead to cybersecurity requirements and priorities that each participant can pursue.

S&T collaborates regularly with DOD's Defense Advanced Research Projects Agency, through connected technical and program reviews and new initiatives discussions. One of these collaborations resulted in a project transfer from the Defense Advanced Research Projects Agency to S&T (Secure Network Attribution and Protection protocol) that was completed in early FY 2015, and this project was evaluated by the U.S. Army Cyber School at Ft. Gordon, Georgia. S&T also works with the Air Force Research Laboratory and Space & Naval Warfare Systems Command organizations to contract parts of its work program, and conducted program familiarization activities with the Air Force Research Laboratory, in particular, in FY 2015. In late FY 2015, S&T began supporting an aviation cybersecurity testing activity that leverages considerable DOD work in this area.

DOD's Countering Terrorism Technical Support Office and S&T are collaborating to launch work on open-source solutions that can be used to improve cybersecurity in technologies ranging from emergency management to unmanned air vehicle operations.

USCG Cooperation with DOD

As a member of the Armed Services, USCG operates on the .mil network and is charged with defending its portion of the DOD Information Network. As such, USCG follows DOD requirements in the performance and operation of its networks and infrastructure. Additionally, USCG takes network defense tasking and direction from USCYBERCOM. Coast Guard Cyber Command serves as the Service Component Command to USCYBERCOM and is designated as the Computer Network Defense Service Provider for USCG. Coast Guard Cyber Command and USCYBERCOM collaborate to mitigate threats to military networks.

In addition to Coast Guard Cyber Command's efforts with USCYBERCOM, 20 USCG personnel are assigned to U.S. Strategic Command; these positions are funded by USCYBERCOM. These positions work at all levels of the organization, including building technical capabilities, conducting cyberspace operations, and deploying in times of conflict to counter cyber threats to national security.

Finally, USCG is a member of the Intelligence Community. As such, USCG units are positioned alongside DOD counterparts to share intelligence and develop technical capabilities to support national intelligence priorities.

USSS Cooperation with DOD

A. Critical Systems Protection

Special agents assigned to the Critical Systems Protection program collaborate closely with members of DOD in direct support of the cybersecurity capability for presidential and vice presidential protection as well for national special security events.

The Critical Systems Protection Program oversees a systematic audit and technical assessment of critical infrastructure and/or utilities that support a protective visit, event, or venue. Critical Systems Protection assessments seek to identify and assess computer networks, process-control systems, or remotely controlled devices that potentially affect an operational security plan if compromised. The result is situational awareness of the overall cybersecurity environment.

The Critical Systems Protection Program has and continues to collaborate closely with Carnegie Mellon University's Software Engineering Institute Computer Emergency Response Team, which is a federally funded research and development center. This collaboration serves to develop the custom technology tool suite that is utilized to support all Critical Systems Protection Program components—Protective Advance and Computer Network Defense capabilities.

B. Cyber Intelligence Section

Special agents assigned to the Cyber Intelligence Section interact daily with members of DOD in direct support of ongoing, transnational network intrusion cases. Cyber Intelligence Section special agents, supported by contracted personnel, analyze structured and unstructured materials derived from USSS criminal investigations, in order to identify key transnational cyber criminals. Such materials include data derived from various investigative actions and sources, such as carding forums (e.g., SQL database dumps), large amounts of data in no particular format, hard drive images, and/or other media that need to be indexed for material to be searchable.

IV. Possible Use of Initiatives at the Secondary and Post-Secondary Levels

Enhancing the security, resilience, and reliability of cyberspace and communications infrastructure for the Nation requires an exceptional workforce. DHS recognizes that recruiting and maintaining this workforce is challenging. The market for cyber talent is competitive, and it is common for both potential recruits and our current employees to receive lucrative employment offers and incentives to join the private sector. DHS's comparative advantage, like other agencies in the Federal Government, is the opportunity to have broad, positive, and lasting impact on issues of national import. Attracting talent includes developing outreach to expose promising candidates at the secondary and post-secondary education levels through programs like Scholarship for Service and the support of student competitions like the Air Force Association's CyberPatriot and the Collegiate Cyber Defense Competition.

The Department's approach toward promoting cybersecurity at the secondary and post-secondary levels addresses:

- Recruitment and Hiring: Recruit cybersecurity professionals of the right quality, at the right levels, at the right rate, and in the right quantity. Consistent with the Office of Personnel Management (OPM), veterans' preference gives eligible veterans preference in appointment over many other applicants. Veterans' preference applies to virtually all new appointments in both the competitive and excepted services.
- Career Development: Provide cybersecurity professionals the experiences, development, training, opportunities, and guidance that they need to support continuous performance improvement and career development.
- Retention and Environment: Ensure that offices are staffed, organized, and structured in a way that supports the utilization, retention, and purposeful succession of cybersecurity and communications professionals.
- Workforce Management: Ensure that supervisors and managers have the skills and competencies necessary to lead the cybersecurity and communications workforce effectively and efficiently.
- Component and Department Level Strategies: Serve as a thought leader and catalyst for driving innovations at the Component and/or Department level that enhance the effectiveness of the cyber workforce.

In addition, providing ongoing training and education opportunities for DHS cybersecurity and communications employees requires a sustained, dedicated, and properly resourced effort. DHS is committed to providing its employees with the tools, training, and tradecraft, to include secondary and post-secondary level opportunities that they need to be successful. This commitment is echoed at the highest levels of Department leadership.

DHS is also a co-sponsor along with the National Science Foundation of the Scholarship for Service program, which provides scholarships to 58 Centers of Academic Excellence-designated universities across the country in specific information assurance degree programs. Students receive Scholarship for Service scholarships for up to 2 years to study cybersecurity, after which they owe the Government a period of service equivalent to the length of their scholarship. Through the *Cybersecurity Enhancement Act* that was signed into law in December 2014, this program provides agencies with greater flexibility and a streamlined method for hiring Scholarship for Service cyber interns. Interns now can be noncompetitively converted into the competitive service after they complete their service requirement. Every year, the Scholarship for Service program holds a job fair that is open only to Scholarship for Service students and hiring managers within federal or state, local, tribal, and territorial governments or federally funded research & development centers.

DHS led development of the National Cybersecurity Workforce Framework (Workforce Framework) and now leads an interagency cybersecurity workforce development working group with members from DOD, the National Institute for Standards and Technology, the Department of Labor, and OPM. Coordination through this working group led to the definition of DOD cyberspace work roles based on the Workforce Framework standard. These work roles form the basis of workforce identification, qualification, and training requirements established in DOD Directive 8140.01, Cyberspace Workforce Management.

Because education is continuous and evolving, other initiatives to promote current cyber learning, training, and development methods, and resources and opportunities are those offered via the online National Initiative for Cybersecurity Careers and Studies portal, Federal Virtual Training Environment and Federal Virtual Training Environment Live! programs. Federal Virtual Training Environment provides federal cybersecurity and information technology professionals with hands-on labs and training courses. Annually, Federal Virtual Training Environment aids in closing training gaps for more than approximately 60,000 cybersecurity professionals across the Federal Government. The environment is accessible from any Internet-enabled computer and is free to users and their organizations. The DHS National Initiative for Cybersecurity Careers and Studies portal (https://niccs.us-cert.gov/) represents a key component that promotes the Workforce Framework, which includes tools and resources for organizations focused on cybersecurity workforce and information for individuals about cybersecurity careers. The National Initiative for Cybersecurity Careers and Studies portal makes resources available to the American public, assisting users of all ages in locating cybersecurity learning opportunities and careers. These include a nationwide training catalogue of cybersecurity training and education resources, a workforce development toolkit that helps employers to establish and manage cybersecurity teams, and guides to help educators develop degrees and curriculum aligned to employer needs. DHS also sponsors the U.S. Cyber Challenge, a collaborative public-private partnership that seeks to help create a pipeline through which talented individuals at the secondary and post-secondary education levels can progress measurably toward a career in cybersecurity. U.S. Cyber Challenge also provides activities concentrating on developing the skills of the individual participant by connecting them with competitions, scholarships, internships, and cyber camps.

Through U.S. Cyber Challenge, DHS also has sponsored the development of CyberCompEx.org, an online community environment that connects the workforce with employers in the cybersecurity industry. CyberCompEx.org allows students to connect with their peers to share knowledge, and provides a platform for students to search for and enroll in competitions and other skill building activities. Additionally, organizations interested in bolstering their workforce with skilled individuals can issue competitions and challenges through CyberCompEx.org as part of the hiring process.

V. Pathways for Veterans to Enter Software Development Programs

The Department's Secretary's Honors Program Cybersecurity Student Volunteer Initiative provides students pursuing cybersecurity-related degrees with an opportunity to work with top DHS cybersecurity professionals, while learning about the unique cybersecurity missions of the Department. Participants complete hands-on projects in a variety of areas, including digital forensics, network diagnostics, and incident response. As part of the promotion of the initiative, the Department focuses on reaching potential veteran applicants and veterans' employment organizations. In 2014, DHS had 70 student volunteers, of whom 13 were veterans. In 2015, DHS had 48 student volunteers, of whom 6 are veterans.

DHS also has invited U.S. veterans to access the Federal Virtual Training Environment, enabling veterans to access online, on-demand cybersecurity training free of charge. This access supports both transitioning veterans' needs for skills that employers demand and the Nation's needs for a skilled and experienced pool of cybersecurity talent. To confirm participants' veteran status, DHS partnered with Hire Our Heroes, a nonprofit organization that verifies applicants' veteran credentials with DOD before granting them access to the Federal Virtual Training Environment. Once verified, these veterans may take unlimited free cybersecurity training through the Federal Virtual Training Environment.

VI. DHS Cyber Workforce

In 2012, the Department created a new reporting process for tracking mission-critical cybersecurity positions performing certain priority tasks; as a result of this inventory process, DHS identified a population of approximately 1,500 federal positions (as of February 2014) performing significant cybersecurity work. DHS expects to have new data available in early FY 2016 about the size of the federal and contractor workforces supporting the Department's cybersecurity mission.

With the passage of P.L. 113-277, the *Border Patrol Agent Pay Reform Act of 2014* (provisions relating to cybersecurity recruitment and retention), and the *Cybersecurity Workforce Assessment Act* (P.L. 113-246), the Department has begun to enhance its cybersecurity workforce planning and analysis activities to meet new statutory reporting requirements and to prepare for the implementation of new human capital authority.

VII. Conclusion

Cooperation between DHS and DOD results in consistent security policies, complementary approaches to countering cyber threats, increased awareness of cyber threats, and uniform requirements for security tools. DHS will continue to leverage the established programs and relationships outlined in this report and continue to incorporate them into an overarching DHS cybersecurity strategy. Further, DHS will continue to foster the cybersecurity relationships that have been developed with DOD, in addition to incorporating them into the overarching strategy for a secure cyberspace.