U.S. Military Cybersecurity-related Provisions Comparison for Fiscal Year 2014

Update 2

U.S. House of Representatives passed FY 2014 National Defense Authorization Act [NDAA] Act (H.R. 1960); U.S. Senate Armed Services Committee passed FY 2014 National Defense Authorization Act [NDAA] Act (S. 1197); U.S. House passed FY 2014 Department of Defense Appropriations bill (H.R. 2397); and the U.S Senate Appropriations Committee proposed FY 2014 Department of Defense Appropriations bill (S. 1429).

There are a plethora of legislative proposals currently being considered in Congress regarding cybersecurity, and certainly more can be expected. These proposals range a broad spectrum of issues dealing with privacy and information sharing to cybercrime offenses and punishment. However, this document only deals with military cybersecurity-related provisions proposed in the FY 2014 NDAA and the FY 2014 Defense Appropriations Act.

Limitation on Availability of Funds for Defensive Cyberspace Operations of the Air Force

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 215 limits the funds the Air Force is able to expend on Defense Cyberspace Operations to no more than 90 percent "until a period of 30 days has elapsed following the date on which the Secretary of the Air Force submits to the congressional defense committees a report on the Application Software Assurance Center of Excellence." The report requires the following to be included:
    - First, a "description of how the Application Software Assurance Center of Excellence is used to support the software assurance activities of the Air Force and other elements of the Department of Defense, including pursuant to section 933 of the National Defense Authorization Act for Fiscal Year 2013."
    - Second, a "description of the resources used to support the Center of Excellence from the beginning of the Center through fiscal year 2014."
    - Third, the "plan of the Secretary for sustaining the Center of Excellence during the period covered by the future-years defense program submitted in 2013 under section 221 of title 10, United States Code."

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Service Credit for Cyberspace Experience or Advanced Education upon original appointment as a Commissioned Officer

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 502 amends Section 533 of title 10, United States Code, the Service credit upon original appointment as a commissioned officer, to include a new sub-section. The new subsection states:

- First, “Under regulations prescribed by the Secretary of Defense, if the Secretary of a military department determines that the number of commissioned officers with cyberspace-related experience or advanced education serving on active duty in an armed force under the jurisdiction of such Secretary is critically below the number needed, such Secretary may credit any person receiving an original appointment with a period of constructive service for the following: (a) Special experience or training in a particular cyberspace-related field if such experience or training is directly related to the operational needs of the armed force concerned; or (b) any period of advanced education in a cyberspace-related field beyond the baccalaureate degree level if such advanced education is directly related to the operational needs of the armed force concerned.”
- Second, “constructive service credited an officer under this subsection shall not exceed one year for each year of special experience, training, or advanced education, and not more than three years total constructive service may be credited.”
- Third, “constructive service credited an officer under this subsection is in addition to any service credited that officer under subsection (a) and shall be credited at the time of the original appointment of the officer.”
- Fourth, “the authority to award constructive service credit under this subsection expires on December 31, 2018.”

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Modification of Requirement for Inventory of Department of Defense Tactical Data Link Systems

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 931 modifies the current requirement for an inventory of Department of Defense tactical data link systems to include “an assessment of vulnerabilities to such systems in anti-access or area-denial environments.”

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Authorities, capabilities, and oversight of United States Cyber Command

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 932 requires the Secretary of Defense to “take such actions as the Secretary considers appropriate to provide the United States Cyber Command operational military units with infrastructure and equipment enabling access to the Internet and other types of networks to permit the United States Cyber Command to conduct its peacetime and wartime missions.”
- Section 932 requires the Secretary of Defense to “review existing cyber ranges and adapt one or more such ranges, as necessary, to support training and exercises of cyber units that are assigned to execute offensive military cyber operations.” Each range, or adapted range, would be required to “have the capability to support offensive military operations against targets that: have not been previously identified and prepared for attack; and must be compromised or neutralized immediately without regard to whether the adversary can detect and attribute the attack.”
- Section 932 requires the Secretary of Defense to “designate, from among the existing personnel of the Office of the Under Secretary of Defense for Policy, a Principal Cyber Advisor to act as the principal advisor to the Secretary on military cyber forces and activities.” The Secretary of Defense could only designate a Principal Cyber Advisor “if such official was appointed to the position in which such official

serves by and with the advice and consent of the Senate." The official designated will have responsibility for:
    - First, "overall supervision of cyber activities related to offensive missions, defense of the United States, and defense of Department of Defense networks, including oversight of policy and operational considerations, resources, personnel, and acquisition and technology."
    - Second, "such other matters relating to offensive military cyber forces as the Secretary shall specify for purposes" of Section 932, subsection (c).
- In addition, the Principal Cyber Advisor will be required to "integrate the cyber expertise and perspectives of appropriate organizations within the Office of the Secretary of Defense, Joint Staff, military departments, Defense Agencies, and combatant commands, by establishing and maintaining a full-time cross-functional team of subject matter experts from those organizations; and select team members, and designate a team leader, from among those personnel nominated by the heads of such organizations." Further, the Joint Explanatory Statement accompanying the FY 2014 NDAA provides additional details regarding its intent:
    - The conferees "stress that this construct of an interdepartmental team under the direction of the principal advisor for cyber is not intended to be merely a coordinating committee," but rather "will provide strong leadership through a joint mechanism to achieve a common purpose and unity of effort in policy, planning, programming, and oversight to support a complex mission that spans the entire Department of Defense." It is the conferees belief that "there are good models for effective cross-functional teams, such as the Joint Inter-Agency Task Force-South, which successfully brings stakeholders together, including their specific authorities and capabilities, under a single organization." Further, "this team concept requires that members operate and think holistically, without regard to home institution loyalties, and receive training in team dynamics and conflict resolution"
    - The Joint Explanatory Statement states that with regard to cyber acquisitions, it notes "that there is an existing congressionally-mandated joint entity, the Cyber Investment Management Board, which is chaired by the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Policy, and the Vice Chairman of the Joint Chiefs of Staff." The conferees "believe such organizations should be leveraged to the extent possible in organizing this cross functional team."
- Section 932 requires the Secretary of Defense to "establish and maintain training capabilities and facilities in the Armed Forces and, as the Secretary considers appropriate, at the United States Cyber Command, to support the needs of the Armed Forces and the United States Cyber Command for personnel who are assigned offensive and defensive cyber missions in the Department of Defense."
- The Joint Explanatory Statement states that conferees "expect the Secretary of Defense to devise means to ensure that CYBERCOM personnel include non-career intelligence and cyber security officers and enlisted personnel with experience in combat arms." Finally, conferees note that they "are aware that there are renewed deliberations about the potential of elevating U.S. Cyber Command from a sub-unified command to a full unified command." In the Joint Explanatory Statement the conferees state that as a part of Section 940 of the FY 2013 NDAA, they "expect to be briefed and consulted on any such proposal at the time when the Secretary of Defense makes such a decision." Further, "as these policy discussion progress," the conferees "expect the department to keep the Committees on Armed Services of the Senate and the House of Representatives informed, upon request, during the quarterly cyber operations briefings, particularly as they relate to the estimated costs and policy implications associated with making the U.S. Cyber Command a unified command."

<u>House Passed FY14 Defense Appropriations (H.R. 2397):</u>

- No similar provision.

<u>SAC Passed FY14 Defense Appropriations (S. 1429):</u>

- No similar provision.

Mission Analysis for Cyber Operations of Department of Defense

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 933 requires a mission analysis for the Department of Defense's cyber operations. Section 933 states, not later than 180 days after the date of the enactment of this Act, the Secretary of Defense is required to "conduct a mission analysis of the cyber operations of the Department of Defense." The mission analysis is required to include:
    - First, the "concept of operations and concept of employment for cyber operations forces."
    - Second, an "assessment of the manpower needs for cyber operations forces, including military requirements for both active and reserve components and civilian requirements."
    - Third, an "assessment of the mechanisms for improving recruitment, retention, and management of cyber operations forces, including through focused recruiting; educational, training, or certification scholarships; bonuses; or the use of short-term or virtual deployments without the need for permanent relocation."
    - Fourth, a "description of the alignment of the organization and reporting chains of the Department, the military departments, and the combatant commands."
    - Fifth, an "assessment of the current, as of the date of the analysis, and projected equipping needs of cyber operations forces."
    - Sixth, "an analysis of how the Secretary, for purposes of cyber operations, depends upon organizations outside the Department, including industry and international partners."
    - Seventh, "methods for ensuring resilience, mission assurance, and continuity of operations for cyber operations."
    - Eighth, an "evaluation of the potential roles of the reserve components in the concept of operations and concept of employment for cyber operations forces, including":
        - "In consultation with the Secretaries of the military departments and the Commander of the United States Cyber Command, an identification of the Department of Defense cyber mission requirements that could be discharged by members of the reserve;"
        - "In consultation with the Secretary of Homeland Security, consideration of ways to ensure that the Governors of the several States, through the Council of Governors, as appropriate, have an opportunity to provide the Secretary of Defense and the Secretary of Homeland Security an independent evaluation of the State cyber capabilities, and State cyber needs that cannot be fulfilled through the private sector;"
        - "An identification of the existing capabilities, facilities, and plans for cyber activities of the reserve components, including: an identification of current positions in the reserve components serving Department cyber missions; an inventory of the existing cyber skills of reserve component personnel, including the skills of unites and elements of the reserve components that are transitioning to cyber missions; an inventory of the existing infrastructure of the reserve components that contributes to the cyber missions of the United States Cyber Command, including the infrastructure available to units and elements of the reserve components that are transitioning to such missions; and an assessment of the manner in which the military departments plan to use the reserve components to meet total force resource requirements, and the effect of such plans on the potential ability of members of the reserve components to support the cyber missions of the United States Cyber Command;"
        - "An assessment of whether the National Guard, when activated in a State status (either State Active Duty or in a duty status under title 32, United States Code) can operate under unique and useful authorities to support domestic cyber missions and requirements of the Department or the United States Cyber Command;"
        - "An assessment of the appropriateness of hiring on a part-time basis non-dual status technicians who possess appropriate cyber security expertise for purposes of assisting the National Guard in protecting critical infrastructure and carrying out cyber missions;"

- "An assessment of the current and potential ability of the reserve components to: attract and retain personnel with substantial, relevant cyber technical expertise who use those skills in the private sector; organize such personnel into units at the State, regional, or national level under appropriate command and control arrangements for Department cyber missions; meet and sustain the training standards of the United States Cyber Command; and establish and manage career paths for such personnel;"
- "A determination of how the reserve components could contribute to total force solutions to cyber operations requirements of the United States Cyber Command;"
- "Development of an estimate of the personnel, infrastructure, and training required, and the costs that would be incurred, in connection with implementing a strategy for integrating the reserve components into the total force for support of the cyber missions of the Department and United States Cyber Command, including by taking into account the potential savings under the strategy through use of" a cyber unit of the Air National Guard of the United States, "provided that for specific cyber units that exist or are transitioning to a cyber mission, the estimate shall examine whether there are misalignments in existing plans between unit missions and facility readiness to support such missions."

- Section 933 also denies any "reduction in personnel of a cyber unit of the Air National Guard of the United States" in FY 2014 "before the submittal of the report" mentioned below. In addition, "no reduction in the personnel or capacity of a Red Team of the Air National Guard of the United States" would authorized "unless the report required" below "includes a certification that the personnel or capacity to be reduced is directly related to Red Team capabilities that are no longer required."
- Further, not later than 30 days after the completion of the mission analysis, the Secretary of Defense is required to submit to Congressional defense committees a report containing: "the results of the missions analysis; and recommendations for improving or changing the roles, organization, missions, concept of operations, or authorities related to the cyber operations of the Department; and any other matters concerning the mission analysis that the Secretary considers appropriate."
- In addition, not later than 30 days after the date on which the Secretary of Defense submits the report, the Chief of the National Guard Bureau is required to submit to the Congressional defense committees an "assessment of the role of the National Guard in supporting the cyber operations mission of the Department of Defense as" such mission is described in the above mentioned report.

<u>House Passed FY14 Defense Appropriations (H.R. 2397):</u>

- The House Committee Report states that "cyber security is an important and growing mission area, and the National Guard has unique access to a wealth of information technology talent within its ranks as well as unique cyber support capabilities associated with both its Federal and State Active Duty statutes." Further, the President's cybersecurity executive order, Improving Critical Infrastructure Cybersecurity, "focuses on enhancing the resiliency and security of the Nation's critical infrastructure," which "will be achieved through a 'partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.'"
- The House Committee Report states that the Committee "recognizes that the National Guard can fill the roles denoted in the President's executive order." The Committee believes that "as dual use, cyber incident response teams, the Guard would focus on forensic analysis and defensive cyber operations, providing all purpose 'triage' of local/state network incidents." In addition, the Committee "recognizes that these Guard teams may provide aid to civil authorities in Title 32, Title 10, and State Active Duty status and should be regionally located near established key infrastructure nodes for the internet to leverage their capabilities."

<u>SAC Passed FY14 Defense Appropriations (S. 1429):</u>

- The Senate Appropriations Committee Report (S. Rept. 113-85) notes that "over the next several years, the military services will be providing additional cyber mission forces to U.S. Cyber Command, composed

of an active duty, civilian, and contractor workforce that has yet to be determined." In addition, the Committee "notes that National Guard and Reserve personnel possess unique skill sets and operate under distinct authorities that could be utilized to meet the national cyber mission force needs." However, the "Department of Defense has not provided the congressional defense committees a comprehensive analysis regarding the role that National Guard and Reserve forces could fulfill as cyber mission forces are established, nor a cost comparison for filling cyber mission forces with active versus Guard and Reserve forces, or a mix thereof."

- Therefore, the Committee would direct "the U.S. Cyber Command, in conjunction with the Office of the Secretary of Defense, to provide to the congressional defense committees no later than 60 days after enactment of this act, a classified and unclassified report" that would include the following:
    - First, "the current number and location of Reserve Component cyber units, as well as skill sets provided by each of these units."
    - Second, "the number of individual teams, their composition by number of personnel, and missions each of the services are establishing for U.S. Cyber Command."
    - Third, "the skill sets required to meet cyber mission team requirements."
    - Fourth, "a cost-benefit-analysis of meeting these requirements with teams comprised of solely active duty personnel, compared to teams partially or fully filled with National Guard or Reserve personnel."
    - Fifth, "an analysis of cyber missions that are being considered for the National Guard and/or Reserves."

Modification of Requirement for Report on Department of Defense Progress in Defending the Department and the Defense Industrial Base from Cyber Events

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 934 of the FY 2014 NDAA amends Section 935 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011. Section 935 of the FY 2011 NDAA requires the Secretary of Defense to annually submit, through 2015, a report on the progress of the Department of Defense in defending the Department and the defense industrial base from cyber events to congressional defense committees. Section 935 of the FY 2011 NDAA outlines three required areas to be covered in the annual report. Section 934 of the FY 2014 NDAA amends the third requirement in the Section 935 report to include "estimated economic impacts" caused by cyber events and "estimates of economic losses resulting from such event."

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Additional Requirements Relating to the Software Licenses of the DoD

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 935 requires the Chief Information Officer of the DoD, in consultation with the chief information officers off the military departments and the Defense Agencies, to "update the plan for the inventory of selected software licenses of the Department of Defense required under section 938 of the National Defense Authorization Act for 2013 to include a plan for the inventory of all software licenses of the Department of Defense for which a military department spends more than $5,000,000 annually on any individual title, including a comparison of licenses purchased with licenses in use." The update is required to:
    - First, "include plans for implementing an automated solution capable of reporting the software license compliance position of the Department and providing a verified audit trail, or an audit trail otherwise produced and verified by an independent third party."
    - Second, "include details on the process and business systems necessary to regularly perform reviews, a procedure for validating and reporting deregistering and registering new software,

and a mechanism and plan to relay that information to the appropriate chief information officer."
    - Third, "a proposed timeline for implementation of the updated plan."
- In addition, not later than September 30, 2015, the Chief Information Officer of the DoD is required to submit to congressional defense committees the updated plan. Further, if the Chief Information Officer of the DoD determines through the implementation of the process and business systems in the updated plan "that the number of software licenses of the Department for an individual title for which a military department spends greater than $5,000,000 annually exceeds the needs of the Department for such software licenses, or the inventory discloses that there is a discrepancy between the number of software licenses purchased and those in actual use, the Chief Information Officer of the Department of Defense shall implement a plan to bring the number of such software licenses into balance with the needs of the Department and the terms of any relevant contract."

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Cyber Outreach and Threat Awareness for Small Businesses

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 937 requires the Secretary of Defense, not later than 60 days after the date of the enactment of this Act, to provide to the House- and Senate-Armed Services Committees "a briefing on options for strengthening outreach and threat awareness programs for small businesses that are awarded contracts by the Department of Defense to assist such businesses to: 1) understand the gravity and scope of cyber threats; 2) develop a plan to protect intellectual property; and 3) develop a plan to protect the networks of such businesses."
- The Joint Explanatory Statement states that conferees "recognize the challenges faced by industry, especially small businesses, when it comes to understanding and defending against advanced cyber threats." The Joint Explanatory Statement notes "there are a number of initiatives and mechanisms within the Department that address aspects of this challenge, such as the Defense Industrial Base Information Assurance/Cyber Security program." However, "because these other efforts exist," the conferees "believe that new programs are not needed." With that said, the conferees do believe "that inadequate attention has been supporting the needs of small businesses, or attempt to measure the strategic effectiveness of those programs."

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Joint Federated Centers for Trusted Defense System for the Department of Defense

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 937 directs the Secretary of Defense to establish a "joint federation of capabilities to support the trusted defense system needs of the Department of Defense." The joint federated centers' purpose would be "to serve as a joint, Department-wide federation of capabilities to support the trusted defense system needs of the Department to ensure security in the software and hardware developed, acquired, maintained, and used by the Department, pursuant to the trusted defense systems strategy of the Department and supporting policies related to software assurance and supply chain risk management." In establishing the federation the Secretary of Defense would be directed to "consider whether the purpose of the federation can be met by existing centers in the Department." And, "if the Department determines that there are capabilities gaps that cannot be satisfied by existing centers, the Department shall devise a strategy for creating and providing resources for such capabilities to fill such gaps." Further, the Secretary of Defense is directed to, not later than 180 days after enactment of this Act, "issue a charter for the federation." The charter would be required to include the following:

    - First, "be established pursuant to the trusted defense systems strategy of the Department and supporting policies related to software assurance and supply chain risk management."
    - Second, "set forth":
        - "the role of the federation in supporting program offices in implementing the trusted defense systems strategy of the Department;"
        - "the software and hardware assurance expertise and capabilities of the federation, including policies, standards, requirements, best practices, contracting, training, and testing;"
        - "the requirements for the discharge by the federation, in coordination with the Center for Assured Software of the National Security Agency, of a program of research and development to improve automated software code vulnerability analysis and testing tools;"
        - "the requirements for the federation to procure, manage, and distribute enterprise licenses for automated software vulnerability analysis tools; and"
        - "the requirements of the discharge by the federation, in coordination with the Defense Microelectronics Activity, of a program of research and development to improve hardware vulnerability, testing, and protection tools."
- A report on the funding and management of the federation would be required to be provided by the Secretary of Defense to the Congressional defense committees at the time of the submittal to Congress of the President's FY 2016 budget. The report shall "set forth such recommendations as the Secretary considers appropriate regarding the optimal placement of the federation within the organizational structure of the Department, including responsibility for the funding and management of the center."
- The Joint Explanatory Statement states that it is the conferees belief "that the trusted defense systems strategy provides a good foundation for guiding the work of these centers in supporting the acquisition and testing community." Further, "as it relates specifically to software assurance," the conferees "note that the DoD is in the process of developing a baseline software assurance policy for the entire life cycle of covered systems in response to section 933 of the National Defense Authorization Act for Fiscal Year 2013." In addition, the conferees "believe that any such guidance and direction for Department program managers should, where possible, and where consistent with adequate security for covered system and the national security, be consistent with recognized standards, and should explore for accepting self-certification or third-party certification for compliance purposes."
- Furthermore, the conferees belief that the "software assurance policy should, where possible, and where consistent with adequate security for covered systems and the national security, be developed in compliance with the Office of Management and Budget Memorandum for Chief Information Officers and Senior Procurement Executive's titled 'Technology Neutrality,' dated January 7, 2011." Finally, the conferees "believe that any future software assurance policy that includes requirements concerning Federal participation in the development and use of voluntary consensus standards should be conducted in accordance with the National Technology Transfer and Advancement Act of 1995, section 272 of title 15, United States Code, and the Office of Management and Budget Circular A-119."

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Supervision of the Acquisition of Cloud Computing Capabilities for Intelligence Analysis

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 938 would require the Secretary of Defense, acting through the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Intelligence, the Chief Information Officer of the Department of Defense, and the Chairman of the Joint Requirements Oversight Council, supervise the following:

    - First, "review, development, modification, and approval of requirements for cloud computing solutions for intelligence data analysis and storage by the Armed Forces and the Defense Agencies, including requirements for cross-domain, enterprise-wide discovery and correlation of data stored in cloud and non-cloud computing databases, relational and non-relational databases, and hybrid databases."
    - Second, "review, development, modification, approval, and implementation of plans for the competitive acquisition of cloud computing systems or services to meet requirements described" above, "including plans for the transition from current computing systems to systems or services acquired."
    - Third, "development and implementation of plans to ensure that the cloud systems or services acquired pursuant to" the above "are interoperable and universally accessible and usable through attribute-based access controls."
    - Fourth, integration of above mentioned plans "with enterprise-wide plans of the Armed Forces and the Department of Defense for the Joint Information Environment and the Defense Intelligence Information Environment."
- The Secretary is directed to provide direction to the Armed Forces and the Defense Agencies on these matters no later than March 15, 2014. In addition, the Secretary of Defense is required to coordinate with the Director of National Intelligence to ensure that activities outlined in Section 938 are integrated with the Intelligence Community Information Technology Enterprise in order to achieve interoperability, information sharing, and other efficiencies. Further, Section 938 will "not apply to a contract for the acquisition of cloud computing capabilities in an amount less than $1,000,000."

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Cyber Vulnerabilities of DoD Weapon Systems and Tactical Communications Systems

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 939 requires the Secretary of Defense to report to Congress, not later than one year after the date of enactment of this Act, "on the status of the capability of each military department to operate in non-permissive and hostile cyber environments." The report is required to include the following:
    - First, "a description and assessment of potential cyber threats or threat systems to major weapon systems and tactical communications systems that could emerge in the next five years."
    - Second, "a description and assessment of cyber vulnerabilities of current major weapons and tactical communications systems."
    - Third, "a detailed description of the current strategy to detect, deter, and defend against cyber attacks on current and planned major weapon systems and tactical communications systems."
    - Fourth, "an estimate of the costs anticipated to be incurred in addressing cyber vulnerabilities to Department of Defense weapon systems and tactical communications systems over the next five years."

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Control and Proliferation of Cyber Weapons

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 940 requires the President to "establish an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative export controls, law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate." Further, the President is required to "include, to the

extent practicable, private industry participation in the process" of establishing an integrated policy to control the proliferation of cyber weapons. The objectives of the interagency process is to:
    - First, "identify the intelligence, law enforcement, and financial sanctions tools that can and should be used to suppress the trade in cyber tools and infrastructure that are or can be used for criminal, terrorist, or military activities while preserving the ability of governments and the private sector to use such tools for legitimate purposes of self-defense."
    - Second, "to establish a statement of principles to control the proliferation of cyber weapons, including principles for controlling the proliferation of cyber weapons that can lead to expanded cooperation and engagement with international partners."
- The interagency process established in Section 940 is required to "develop, by not later than 270 days after the date of the enactment of this Act, recommendations on means for the control of the proliferation of cyber weapons, including a draft statement of principles and a review of applicable legal authorities."

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Integrated Policy to Deter Adversaries in Cyberspace

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 941 requires the President to "establish an interagency process to provide for the development of an integrated policy to deter adversaries in cyberspace." The objective of the interagency process is "to develop a deterrence policy for reducing cyber risks to the United States" and its allies. Section 941 requires that the President to "submit to the congressional defense committees a report setting forth the integrated policy developed," not later than 270 days after the date of the enactment of this Act.

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

National Centers of Academic Excellence in Information Assurance Education Matters

FY 2014 National Defense Authorization Act (H.R. 3304):

- Section 942 directs that "each institution of higher education that was designated by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Information Assurance Education as of January 1, 2013, shall continue to be designated as such a Center through June 30, 2015, provided that such institution maintains the standards by which such institution was originally designated as such a Center."
- Section942 requires the Secretary of Defense, not later than 180 days after the date of the enactment of this Act, in consultation with the Secretary of Homeland Security, the Director of the National Security Agency, and other appropriate departments and agencies of the Federal Government and non-Federal organizations, to:
    - First, "assess the National Centers of Academic Excellence in Information Assurance Education program strengths and weaknesses, including processes and criteria used to develop curricula and designate an institution of higher education as a National Center of Excellence in Information Assurance Education."
    - Second, "assess the maturity of information assurance as an academic discipline."
    - Third, "assess the role the Federal Government should play in the future development of curricula and other criteria for designating or accrediting information assurance education programs of institutions of higher education as National Centers of Academic Excellence in Information Assurance Education."
    - Fourth, "assess the advantages and disadvantages of broadening the governance structure of such Centers."

    - Fifth, “assess the extent to which existing and emerging curricula and other criteria for designation as such a Center is aligned with the National Initiative for Cybersecurity Education and will provide the knowledge and skills needed by the information assurance workforce for existing and future employment.”
    - Sixth, “make recommendations for improving and evolving the mechanisms and processes for developing the curricula and other criteria for accrediting or designating information assurance programs of institutions of higher education as Centers.”
    - Seventh, “make recommendations on transitioning the responsibility for developing the curricula and other criteria for accrediting or designating information assurance programs of institutions of higher education as Centers from the sole administration of the National Security Agency.”
- Section 942 directs the Secretary of Defense, not later than 180 days after the date of the enactment of this Act, to assess the collaboration of the Department of Defense with the National Centers of Academic Excellence in Information Assurance Education. The assessment is required to include:
    - First, “the extent to which the information security scholarship program of the Department of Defense” contributes to: “building the capacity to education the information assurance and cybersecurity workforce needed for the future; and employing exceptional information assurance and cybersecurity works in the Department of Defense.”
    - Second, “mechanisms for increasing Department employment of graduates of such Centers.”
- Section 942 directs the Secretary of Defense, not later than one year after the date of the enactment of this Act, in consultation with the Secretary of Homeland Security, the Director of the National Security Agency, and other appropriate departments and agencies of the Federal Government and non-Federal organizations, to submit to Congress a:
    - First, “a plan for implement the recommendations made” in the above mentioned assessment and recommendation of accreditation or designation process “on improving and evolving the mechanisms and processes for developing the curricula and other criteria for accrediting and esginating the information assurance programs of institutions of higher education as National Centers of Academic Excellence in Information Assurance Education.”
    - Second, the results of the assessment and recommendation of accreditation or designation process and the assessment of DoD collaboration with Centers.
    - Third, the recommendations made in the assessment and recommendation of accreditation or designation process.
- Finally, “in developing the plan” to implement the recommendations, the Secretary of Defense is required to “consult with appropriate representatives of information assurance interests in departments and agencies of the Federal Government, State and local governments, academia, and the private sector.”

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

Cybersecurity of Space Assets

FY 2014 National Defense Authorization Act (H.R. 3304):

- No similar language.

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar language.

SAC Passed FY14 Defense Appropriations (S. 1429):

- The Senate Appropriations Committee Report (S. Rept. 113-85) states that the “Committee understands it is an Army priority to augment its capability for cybersecurity research on net-centric embedded weapon systems and to research and evaluate technologies for space-based and cyberspace applications for Army tactical ground forces.” Further, the “Army’s strategic forces mission requirements

include maintaining Army force modernization in space." Therefore, the Committee would encourage "the Army to apply the appropriate resources to ensure cyberspace technologies research for the security of space assets, which in turn ensures" the United States "warfighters can receive critical information in a battlefield environment." In addition, the Committee suggest "leveraging existing personnel and recently acquired technology development management programs" as a way to "provide services such as mitigation strategies to agencies that develop, acquire, and maintain space and net-centric weapons assets, to include the Missile Defense Agency."

Army Cyber Forces Footprint

FY 2014 National Defense Authorization Act (H.R. 3304):

- No similar provision.

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- The Senate Appropriations Committee Report (S. 113-85) notes that "Army cyber forces are currently dispersed throughout the continental United States, with key elements co-located with U.S. Cyber Command, and other service cyber components, which allows for significant synergies and operational efficiencies." In addition, the Committee "understands that the Army is currently reviewing its cyber forces footprint." Further, "following conversations with Army leadership, the Committee understands that these discussions are preliminary, and that no funds are included in the fiscal year 2014 budget request to modify or move the Army's cyber missions." Therefore, the Committee would direct "the Army to brief the congressional defense committees on any proposed adjustments to the Army's cyber footprint, to include the associated training, infrastructure and sustainment costs."

Training Standards for Department of Defense Cyber Missions

FY 2014 National Defense Authorization Act (H.R. 3304):

- No similar provision.

House Passed FY14 Defense Appropriations (H.R. 2397):

- No similar provision.

SAC Passed FY14 Defense Appropriations (S. 1429):

- The Senate Appropriations Committee Report (S. Rept. 113-85) notes that the "expansion of cyber mission forces requires extensive training of personnel to meet the needs identified by U.S. Cyber Command." Further, "each of the services provides personnel with different skill sets and knowledge levels, and therefore generate different skill sets and knowledge levels, and therefore generate different training requirements." Therefore, the Committee would direct the "U.S. Cyber Command, in conjunction with the Secretary of Defense, to provide to congressional defense committee," not later than 90 days after enactment of S. 1429, a classified and unclassified report that would include:
    - First, "an identification and analysis of training requirements necessary to meet U.S. Cyber Command cyber mission personnel initial and full operational capability."
    - Second, "a roadmap of training to be provided to active duty and Guard and Reserve personnel to meet those requirements."
    - Third, "cost estimates by service and mission team to meet training requirements for each cyber mission team."
    - Fourth, "an estimated timeline to complete the training required to reach full operational capability of the cyber mission teams, as proposed in the fiscal year 2014 budget."
- In addition, the Committee recognizes "the limitations in existing training resources to meet cyber mission force training requirements in the near-term."
- Therefore, the Committee would recommend "that the military services analyze existing training opportunities and infrastructure, taking into account existing facilities and pre-existing synergies with the Department of Defense and Intelligence Community when establishing their training programs." Further, the Committee would direct "U.S. Cyber Command to provide to the congressional defense

committees" not later than 90 days after enactment of S. 1429, "an analysis of U.S. Government cyber mission force training infrastructure."

Cyber Command Funding

FY 2014 National Defense Authorization Act (H.R. 3304):

- No similar provision.

House Passed FY14 Defense Appropriations (H.R. 2397):

- Funding for the United States Cyber Command, a subordinate unified command under the United States Strategic Command, currently is not discretely visible in the Air Force's budget justification material. With the increased emphasis on cyber activities and related resourcing, the Committee directs that beginning in fiscal year 2015, the Air Force's budget justification material separately report and separately justify funds to support Cyber Command in sub-activity group -15A, "Combatant Commands Direct Mission Support" and in sub-activity group -15B, "Combatant Command Core Operations."

SAC Passed FY14 Defense Appropriations (S. 1429):

- No similar provision.

About the Space Foundation

The foremost advocate for all sectors of the space industry and an expert in all aspects of space, the Space Foundation is a global, nonprofit leader in space awareness activities, educational programs that bring space into the classroom and major industry events, including the *National Space Symposium*, all in support of its mission "to advance space-related endeavors to inspire, enable and propel humanity." The Space Foundation publishes *The Space Report: The Authoritative Guide to Global Space Activity* and provides three indexes that track daily U.S. stock market performance of the space industry. Through its Space Certification™ and Space Technology Hall of Fame® programs, the Space Foundation recognizes space-based technologies and innovations that have been adapted to improve life on Earth. The Space Foundation was founded in 1983 and is based in Colorado Springs, Colo. Its world headquarters features a public Visitors Center with two main areas - the El Pomar Space Gallery and the Northrop Grumman Science Center featuring Science On a Sphere®. The Space Foundation also conducts research and analysis and government affairs activities from its Washington, D.C., office and has a field office in Houston, Texas. For more information, visit www.SpaceFoundation.org. Follow us on Facebook, LinkedIn and Twitter, and read about the latest space news and Space Foundation activities in *Space Watch*.