The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security

‚name redacted,
Analyst in Government Organization and Management

‚name redacted,
Analyst in American National Government

January 8, 2016

Congressional Research Service
7-....
www.crs.gov
R44364

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The federal cybersecurity workforce is responsible for protecting U.S. government systems and networks against cyber threats and attacks. Federal agencies, however, have reported difficulty in assessing the size and capabilities of their cybersecurity workforces. DOD and DHS, which play prominent roles in the nation's cybersecurity posture, have also noted certain obstacles affecting the recruitment and retention of qualified cybersecurity professionals to fulfill their departments' cybersecurity missions.

The Office of Personnel Management (OPM) is constructing a dataset to catalog all federal cybersecurity positions in the executive branch. The dataset had not been released to Congress or the public. In addition, the Office of Management and Budget (OMB) directed agencies to identify their top five cyber talent gaps by December 31, 2015. Congress has also authorized hiring and pay flexibilities that can be used to fill cybersecurity positions at DOD and DHS. The flexibilities aim to enhance the recruitment and retention of cybersecurity professionals by expediting the federal hiring process and providing such professionals with monetary incentives that are not available to all federal employees. OPM has also established temporary hiring flexibilities for certain DOD and DHS cybersecurity positions.

Congress, pursuant to its oversight authority, might seek to increase its awareness and knowledge of these initiatives. OPM is not required to report to Congress on agencies' progress in coding their federal cybersecurity positions or in completing the agency's cybersecurity dataset. Further, DOD and DHS are not required to report on the use or effectiveness of certain hiring and pay flexibilities for cybersecurity positions. Congress may find it difficult to identify potential implementation issues, such as (1) conflicting efforts to define and identify the federal cybersecurity workforce, (2) discrepancies between the intended and actual use of hiring and pay flexibilities, and (3) measuring the overall effectiveness of the flexibilities.

Congress could consider enhancing its oversight of executive branch initiatives to define and identify federal cybersecurity positions by (1) requiring OPM to notify Congress of its progress on completing the cybersecurity dataset, and (2) directing the Government Accountability Office (GAO) to evaluate the operation and effectiveness of the cybersecurity workforce dataset upon its completion. Congress could also enhance its oversight of the implementation of hiring and pay flexibilities for DOD and DHS by (1) conforming reporting requirements among the three laws governing hiring and pay flexibilities, (2) requiring additional reporting on the use of certain flexibilities, (3) directing DOD and DHS, or GAO, to evaluate the effectiveness of the hiring and pay flexibilities, and (4) requiring DOD and DHS human resources staff to receive training on the structure and operation of the flexibilities.

Contents

Figures

Tables

Appendixes

Contacts

Introduction

Cybersecurity refers to a broad set of concepts for which there is no standard definition—it often varies by the entity employing it. DHS, for example, has defined cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[1] The Committee on National Security Systems has defined a "cyber attack" as

> An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.[2]

Strengthening federal cybersecurity has been a priority for Congress and the executive branch for several years.[3] The focus on cybersecurity has increased since the Office of Personnel Management (OPM) data intrusion was revealed in June 2015, which heightened concerns about vulnerabilities within the government's systems and networks.[4]

All federal agencies have responsibilities for protecting their individual systems and networks under federal law.[5] Some agencies, such as DHS and DOD, possess broader cybersecurity roles compared to other agencies. DHS has responsibility for protecting unclassified federal civilian systems and networks and assisting agencies in responding to cyber threats and attacks.[6] DHS is also the lead agency for coordinating with the private sector to protect critical cyber infrastructure assets.[7] DOD is responsible for defending the nation against cyberattacks of "significant consequence," as well as conducting military operations in cyberspace.[8] DOD is also responsible for assisting DHS in fulfilling its government-wide cybersecurity roles.[9]

---

[1] U.S. Department of Homeland Security (hereinafter DHS) "Explore Terms: A Glossary of Common Cybersecurity Terminology," at https://niccs.us-cert.gov/glossary. For more information on the definition of cybersecurity, see CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by (name redacted)

[2] Committee on National Security Systems, *National Information Assurance Glossary*, CNSS Instruction No. 4009, April 26, 2010, p. 22, at http://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf.

[3] The U.S. Government Accountability Office (hereinafter GAO) added "security of federal cyber assets" to its high-risk list in 1997, and has since added protecting cyber critical infrastructure (2003) and the personally identifiable information (2015). See GAO, "High Risk List, Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information," February 2015, at http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study#t=0.

[4] For more information on the OPM data intrusion, see CRS Report R44111, *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, coordinated by (name redacted)

[5] CRS has compiled a list of laws that govern the federal role in cybersecurity. See CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by (name redacted)

[6] DHS, "Preventing and Defending Against Cyber Attacks," October 2011, at http://www.dhs.gov/xlibrary/assets/preventing-and-defending-against-cyber-attacks-october-2011.pdf.

[7] Executive Office of the President, "Executive Order—Improving Critical Infrastructure Cybersecurity," February 12, 2013, at https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; Executive Office of the President, "Presidential Policy Directive—Critical Infrastructure Security and Resilience," February 12, 2013, at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[8] U.S. Department of Defense (hereinafter DOD), *National Military Strategy for Cyberspace Operations*, December 2006, PDF p. 14, at http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf; DOD, *The DOD Cyber Strategy*, April 2015, pp. 4-5 and 25, at http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. Examples of attacks of significant consequence (continued...)

The federal cybersecurity workforce plays an integral role in maintaining and improving the government's cybersecurity. Cybersecurity professionals[10] are responsible for designing and building secure information networks and systems, identifying and addressing vulnerabilities within those networks and systems, and collecting and analyzing data necessary to respond to cyberattacks efficiently and effectively, among other things. Federal stakeholders and researchers have stated that robust federal cybersecurity is not possible without cybersecurity professionals.[11]

Developing and maintaining a robust federal cybersecurity workforce, however, has been an ongoing challenge. The Chief Human Capital Officers Council Working Group found skills gaps in cybersecurity positions (and other positions) government-wide, which prompted the Obama Administration to create a Cross-Agency Priority (CAP) to reduce those gaps by half by the end of FY2013.[12] According to a January 2015 GAO report, however, efforts to close these cybersecurity gaps were at an "early stage of maturity."[13]

This report examines congressional oversight of two strategies undertaken by Congress and the executive branch to strengthen the federal cybersecurity workforce: (1) initiatives to define and identify the federal cybersecurity workforce, and (2) hiring and pay flexibilities applicable to cybersecurity positions at DOD and DHS. This report focuses on DOD and DHS because of their key roles in federal cybersecurity and because the majority of hiring and pay flexibilities for cybersecurity professionals authorized by Congress apply to DOD and DHS.

Background on the Federal Cybersecurity Workforce

Defining the Federal Cybersecurity Workforce

Cybersecurity functions are embedded within a wide range of federal positions that span more than 100 federal occupational series (see the text box below for a definition of occupational series).[14] The specific cybersecurity functions undertaken within an occupation series often vary by agency. For example, one DHS position in the 2210 occupation series that performs cybersecurity functions is responsible for identifying vulnerabilities and weaknesses within IT

(...continued)

include those that can result in the loss of life or serious economic impact to the United States.

[9] Ibid. For more information on DOD's cybersecurity responsibilities, see CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by (name redacted) .

[10] The terms "cybersecurity professional" and "cybersecurity employee" are used interchangeably in this report.

[11] See, for example, GAO, *Cybersecurity Human Capital, Initiative Need Better Planning and Coordination*, November 2011, p. 3, at http://www.gao.gov/assets/590/586494.pdf.

[12] GAO, "High Risk List, Strategic Human Capital Management," at http://www.gao.gov/highrisk/strategic_human_management/why_did_study#t=1; Executive Office of the President, "Cross-Agency Priority Goal, Closing Skills Gaps, FY2013 Q4 update," pp. 1-2, at http://goals.performance.gov/content/closing-skills-gaps. The CAP goal included other mission-critical occupations identified as facing skills gaps, such as acquisition and economist positions.

[13] GAO, *Federal Workforce, OPM and Agencies Need to Strengthen Efforts to Identify and Close Mission-Critical Skills Gaps*, GAO-15-223, January 2015, p. 15, at http://www.gao.gov/assets/670/668202.pdf.

[14] OPM, "A Strategic Perspective on the Federal Cybersecurity Work Function," November 2014, p. 10, at https://www.fbcinc.com/e/nice/ncec/presentations/NICE2014_Antone.pdf.

systems and developing procedures to defend against unauthorized access to the systems.[15] A different DHS position in the 2210 occupation series that performs cybersecurity functions, in contrast, is responsible for evaluating and responding to cyber incidents.[16]

OPM Occupational Series

An occupation series includes groups of federal positions that perform similar work and require similar qualifications. For example, the Information Technology (IT) Management occupation series (2210) includes positions that "manage, supervise, lead, administer, develop, deliver, and support information technology systems and services" and require knowledge of IT principles, concepts, and methods.[17] A 2011 GAO report on the federal cybersecurity workforce identified several occupational series that typically undertake cybersecurity responsibilities, including (but not limited to) information technology management, general engineering, and intelligence.[18]

The full range of federal positions that undertake cybersecurity responsibilities is challenging to assess. Researchers have found that agencies have experienced difficulty in accurately defining and measuring their cybersecurity workforces.[19] For example, a 2011 GAO report found wide disparities in counts of DOD cybersecurity employees—88,159 employees reported by GAO, compared to 18,955 reported by OPM. The GAO report partly attributed these inconsistent counts to the lack of a standard definition of a cybersecurity employee.[20]

Challenges to Developing and Maintaining the Workforce

Federal stakeholders and researchers have reported ongoing challenges to developing and maintaining a robust federal cybersecurity workforce. Commonly reported challenges are listed below and include government-wide and agency-specific concerns:

- demand outstripping supply for cybersecurity professionals in the federal government and difficulty filling vacant cybersecurity positions;[21]
- skills gaps in cybersecurity positions;[22] and

[15] The vacancy announcement for the position is closed, but as of January 8, 2016, could still be viewed at https://www.usajobs.gov/GetJob/PrintPreview/412242100.

[16] The vacancy announcement for the position is closed, but as of January 8, 2016, could still be viewed at https://www.usajobs.gov/GetJob/PrintPreview/412534800.

[17] OPM, "Handbook of Occupational Groups and Families," May 2009, pp. 120-121, at https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/occupationalhandbook.pdf.

[18] GAO, *Cybersecurity Human Capital, Initiatives Need Better Planning and Coordination,* GAO-12-8, November 29, 2011, p. 14.

[19] See, for example, ibid., pp. 12-13 and 15.

[20] Ibid., p. 13 and 15. The OPM count was conducted in 2010, whereas the GAO count was conducted in 2011. It is unclear if the OPM statistic included contractors. Research has indicated that contractors perform a notable proportion of cybersecurity work for agencies. For example, data from an OMB report indicated that approximately 33% of "IT Security" FTEs at agencies were contractors. For more information, see OMB, *Report to Congress on Implementation of the Federal Information Security Management Act of 2002,* March 2013, p. 55, at https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

[21] RAND Corporation, "Shortage of Cybersecurity Professionals Poses Risk to National Security," June 18, 2014, at http://www.rand.org/news/press/2014/06/18.html. Partnership for Public Service, *Cyber In-Security II, Closing the Federal Talent Gap,* April 2015, pp. 1 and 10. GAO, *Cybersecurity Human Capital, Initiatives Need Better Planning and Coordination,* GAO-12-8, November 29, 2011, pp. 20-21. RAND indicated that demand will likely be met over time due to an increased number of cybersecurity training and education programs. The GAO report notes that some agencies were able to fill needed cybersecurity positions, while others experienced challenges to filling such positions.

[22] GAO, *Federal Workforce: OPM and Agencies Need to Strengthen Efforts to Identify and Close Mission-Critical Skills Gaps*, GAO-15-223, January 30, 2015, pp. 2 and 15.

- agency strategic workforce plans that do not specifically address cybersecurity workforce needs.[23]

DOD and DHS have reported recruitment and retention challenges for their cybersecurity workforces, including an inadequate number of qualified cybersecurity professionals.[24] DOD and DHS have partly attributed these challenges to the following factors:

- **Federal hiring process** – DOD noted that the length and complexity of the hiring process may deter cybersecurity professionals from pursuing federal careers.[25]
- **General Schedule (GS) pay system** – DHS and other agencies believed that the GS system placed them at a competitive disadvantage for attracting cyber talent, noting that other agencies using non-GS systems were able to pay cybersecurity professionals higher salaries.[26]
- **Federal security clearance process** – DOD and DHS cited the amount of time required to obtain security clearances for new employees as a barrier to filling cybersecurity positions.[27]

Executive Branch Efforts to Define and Identify the Federal Cybersecurity Workforce

The executive branch has several initiatives to define and identify the federal cybersecurity workforce: (1) the national cybersecurity workforce framework, (2) cybersecurity data codes, and (3) a federal cybersecurity workforce dataset. Laws aiming to define and identify the workforce mandate the use of these initiatives.

The National Cybersecurity Workforce Framework

In November 2011, the National Initiative for Cybersecurity Education (NICE), within the National Institute of Standards and Technology (NIST), released the national cybersecurity workforce framework.[28] The framework provides a consistent way to define and describe

[23] GAO, *Cybersecurity Human Capital, Initiatives Need Better Planning and Coordination*, GAO-12-8, November 29, 2011, pp. 8-11.

[24] Ibid., p. 21; GAO, *Defense Department Cyber Efforts, DOD Faces Challenges In Its Cyber Activities*, GAO-11-75, July 2011, pp. 8-9, at http://www.gao.gov/assets/330/321818.pdf; GAO, *Cybersecurity Human Capital, Initiatives Need Better Planning and Coordination*, GAO-12-8, November 29, 2011, p. 21; GAO, *DHS Is Generally Filling Mission-Critical Positions, But Could Better Track Costs of Coordinated Recruiting Efforts*, GAO-13-742, September 2013, p. 24, at http://gao.gov/assets/660/657902.pdf; Homeland Security Advisory Council, *CyberSkills Task Force Report*, Fall 2012, p. 5, at https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf.

[25] GAO, *Cybersecurity Human Capital, Initiatives Need Better Planning and Coordination*, GAO-12-8, November 29, 2011, pp. 21-22.

[26] Ibid., pp. 29-30.

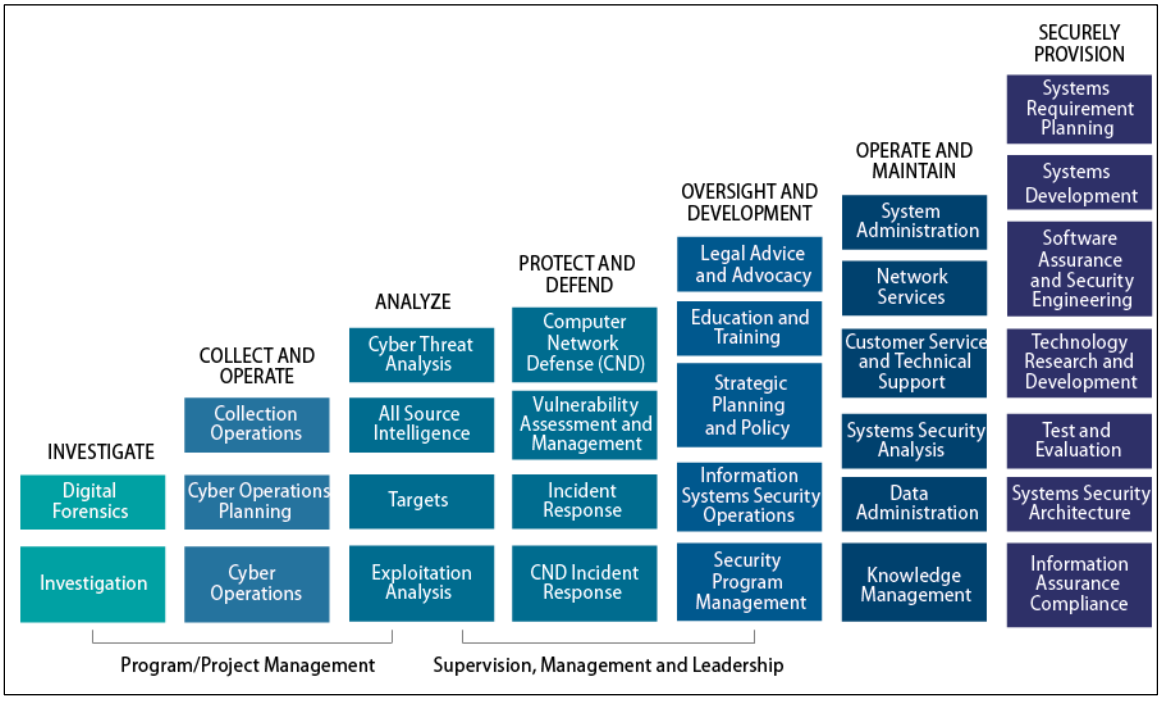
[27] Ibid. pp. 24-25; GAO, *DHS Is Generally Filling Mission-Critical Positions, But Could Better Track Costs of Coordinated Recruiting Efforts*, GAO-13-742, September 2013, p. 24. For more information on the federal security clearance process, see CRS Report R43216, *Security Clearance Process: Answers to Frequently Asked Questions*, by (name redacted) and (name redacted) .

[28] National Institute of Standards and Technology (hereinafter NIST), "NICE Issues Cybersecurity Workforce Framework for Public Comment," November 8, 2011, at http://www.nist.gov/itl/cyberwork-110811.cfm.

cybersecurity work at any public or private organization, including federal agencies.[29] The framework classifies and categorizes cybersecurity work under specialty areas, which are grouped into seven categories (**Figure 1** illustrates these specialty areas and categories).[30] Within each specialty area, the framework defines standard duties and competencies for cybersecurity professionals, as well as job titles that typically involve such duties.

Figure 1. The National Cybersecurity Workforce Framework

(as illustrated by the Partnership for Public Service)



Source: The figure is excerpted from Partnership for Public Service, *Cyber In-Security II, Closing the Federal Talent Gap,* April 2015, p. 8.

Cybersecurity Data Codes

In October 2012, OPM, in coordination with NIST, published a coding structure for federal cybersecurity positions based on the national cybersecurity workforce framework.[31] The structure assigns unique numeric codes to each of the seven categories and specialty areas within the framework and three new categories not included in the framework: (1) Cybersecurity Program/Project Management; (2) Cybersecurity Supervision, Management, and Leadership; and (3) Not Applicable.[32] The codes are intended to allow OPM and agencies to identify and

[29] DHS, National Initiative for Cybersecurity Careers and Studies (hereinafter NICCS), "National Cybersecurity Workforce Framework," at https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework. The framework was developed in collaboration with other federal agencies and private sector representatives.

[30] DHS, NICCS, "National Cybersecurity Workforce Framework," at https://niccs.us-cert.gov/training/tc/framework.

[31] OPM, "The Use and Usefulness of the Cybersecurity Data Element," December 6, 2012, PDF p. 2, at http://csrc.nist.gov/groups/SMA/forum/documents/december2012presentations/dec2012_cybersec_data_element.pdf.

[32] OPM, *The Guide to Data Standards, Part A: Human Resources,* November 15, 2014, PDF pp. 104-110, at http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf. The guide includes procedures on how to properly assign the data codes to federal positions.

categorize all federal cybersecurity positions,[33] thereby laying the groundwork for a consistent government-wide count of the federal cybersecurity workforce.

Federal Cybersecurity Workforce Dataset

In June 2013, OPM launched an initiative to build and use a comprehensive dataset of existing and future executive branch cybersecurity positions.[34] The initiative, known as the Special Cybersecurity Workforce Project, was created to support the FY2013 Cross-Agency Priority (CAP) goal to close cybersecurity workforce skills gaps.[35] The project includes three phases:

1. *build* a dataset of all federal cybersecurity positions,
2. *assess* the accuracy of data contained therein, and
3. *use* the dataset to identify and address needs of the federal cybersecurity workforce.[36]

To support construction of the dataset, OPM directed agencies to assign OPM cybersecurity data codes to their positions. As of November 2015, roughly 95% of *all* federal positions (not just cybersecurity positions), and 96% of positions in the 2210 occupation series, had been assigned an OPM cybersecurity data code.[37] The OPM dataset, as well as a government-wide count of the federal cybersecurity workforce, however, has not been released to the public. OPM staff did not indicate when the dataset would be available on OPM's online workforce data portal, noting that the release date will depend on the accuracy of the data.[38]

Cybersecurity Workforce Skills Gap Assessments

On October 30, 2015, OMB issued the Cybersecurity Strategy and Implementation Plan (CSIP).[39] The CSIP directs agencies to, among other things, complete the following activities to identify skills gaps in the federal cybersecurity workforce:

1. All agencies—identify their top five cyber talent gaps using OPM's cybersecurity dataset.[40]
2. OPM, DHS, and OMB—issue a report that maps "the entire cyber workforce landscape across all agencies using the NICE national cybersecurity workforce framework and identify cyber talent gaps and recommendations for closing them."[41]

[33] Ibid., PDF p. 104.

[34] OPM, memorandum from Elaine Kaplan, OPM Acting Director, to the heads of executive departments and agencies, "Special Cybersecurity Workforce Project," July 8, 2013, at https://www.chcoc.gov/content/special-cybersecurity-workforce-project.

[35] Ibid.

[36] OPM, "A Strategic Perspective on the Federal Cybersecurity Work Function," November 2014, pp. 4 and 6.

[37] Information provided to CRS from OPM staff via email on November 17, 2015.

[38] Ibid.

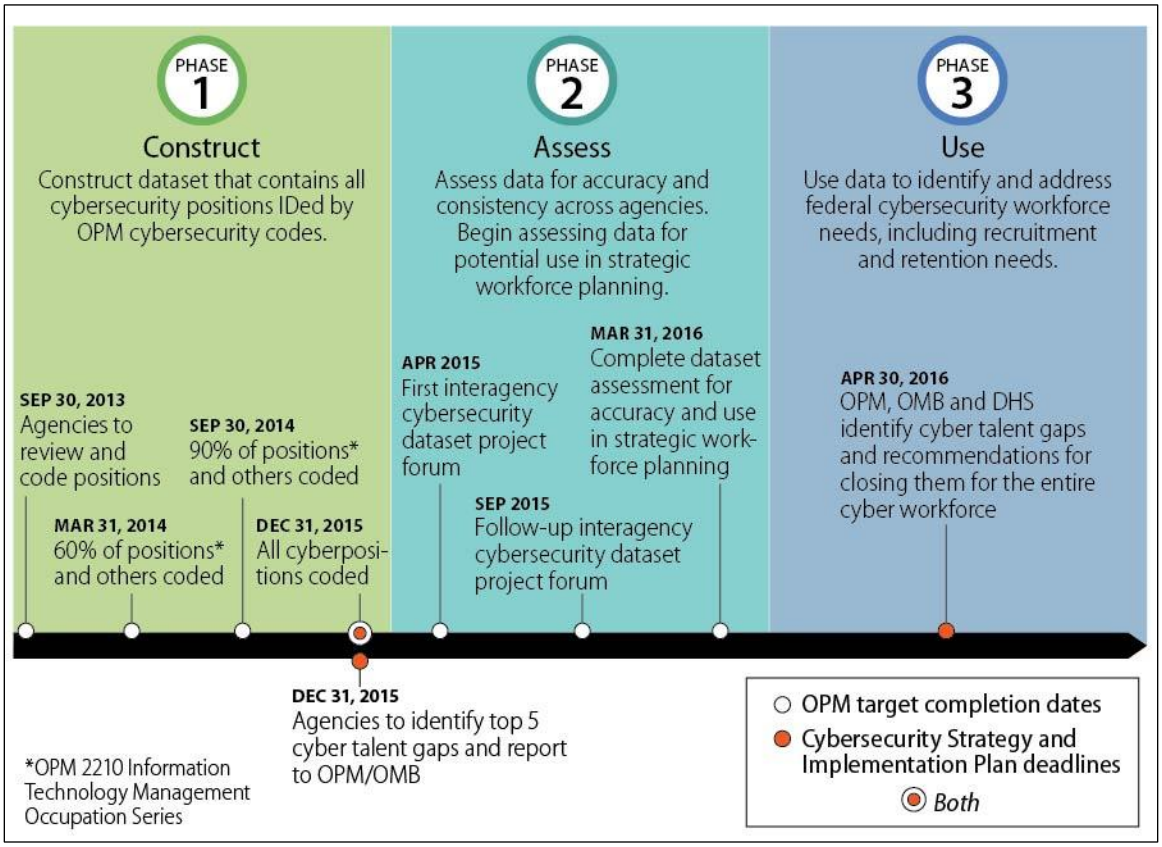
[39] U.S. Office of Management and Budget (hereinafter OMB), memorandum from Shaun Donovan, Director of OMB, and Tony Scott, Federal Chief Information Officer, to the Heads of Executive Departments and Agencies, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," M-16-04, October 30, 2015, at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

[40] Ibid., p. 18.

[41] Ibid., p. 19.

Figure 2, below, includes key activities for OPM's cybersecurity dataset initiative and related CSIP activities. OPM has completed Phase 1, anticipates completing Phase 2 by March 31, 2016, and anticipates beginning Phase 3 during the "latter part of FY2016."[42] These CSIP activities may accelerate planned implementation of Phase 3, as they require agencies to use the dataset for workforce planning purposes.

Figure 2. Timeline for Building and Using OPM's Cybersecurity Dataset



Source: CRS analysis of OPM Special Cybersecurity Workforce Project documents and OMB's Cybersecurity Strategy and Implementation Plan (CSIP); information provided to CRS from OPM staff via email on July 28, 2015, and November 17, 2015.

Notes: The graphic includes certain activities from the CSIP, which are not part of OPM's original goals for the dataset initiative. The graphic is not exhaustive and may not capture the full range of activities for each phase.

Efforts to Define and Identify the Federal Cybersecurity Workforce Through Legislation

Two laws include provisions that aim to define and identify federal cybersecurity positions:

1. The Border Patrol Pay Agent Reform Act of 2013 (P.L. 113-277)[43]
2. The Consolidated Appropriations Act, 2016 (P.L. 114-113)[44]

[42] Information provided to CRS from OPM staff via email on November 17, 2015.

[43] Enacted on December 18, 2014.

The laws codify, and in some ways enhance, OPM's ongoing efforts to define and code federal cybersecurity positions since 2013. The laws also enhance OMB's efforts to assess agencies' cybersecurity workforce capabilities. Broadly, the laws require all agencies to (1) assign data codes to all cybersecurity positions according to the national cybersecurity workforce framework; (2) conduct critical needs assessments for identified cyber positions; and (3) submit progress reports on completing these tasks. **Table 1**, below, compares efforts to define, identify, and assess federal cybersecurity positions between the laws and the OPM/OMB directives described above.

Table 1. Comparison of Laws and OPM/OMB Efforts to Identify, Code, and Assess Federal Cybersecurity Positions

Requirement	OPM directive (Jul 2013)	P.L. 113-277, Sec. 4 (Dec 2014)	OMB directive (Oct 2015)	P.L. 114-113, Division N, Title III (Dec 2015)
Identification & coding	Agencies to assign OPM cybersecurity data codes to all cybersecurity positions by December 31, 2015.	DHS to assign OPM cybersecurity data codes to all cybersecurity positions no later than *nine months* after the date of enactment (September 2015).	Agencies to participate in OPM's cybersecurity dataset project and report all cybersecurity positions to OPM by December 31, 2015.	Agencies to assign OPM cybersecurity data codes, in coordination with NIST, to all cybersecurity positions no later than *one year* after the establishment of code assignment procedures.
Baseline skills assessment	No requirement.	No requirement.	No requirement.	Provide baseline skills assessments of agencies' cybersecurity workforces, including (1) the percentage of cybersecurity employees who possess appropriate industry-recognized certifications for their positions, (2) the level of preparedness of cybersecurity employees without credentials to acquire them, and (3) a strategy for mitigating gaps within these two areas.

(...continued)

[44] Enacted on December 18, 2015. The workforce provisions were included in Division N of Title III within the Consolidated Appropriations Act, 2016, titled the Federal Cybersecurity Workforce Assessment Act of 2015. The Federal Cybersecurity Workforce Assessment Act of 2015 originated in S. 2007 (114th Congress), which was introduced by Senator Bennett on August 6, 2015. Language from S. 2007 was subsequently included in Title III of the Cybersecurity Information Sharing Act of 2015 (S. 754), which passed the Senate by a roll call vote of 74-21 on October 27, 2015. An amended version of S. 754 was included in Title III of Division N of the Consolidated Appropriations Act, 2016.

Requirement	OPM directive (Jul 2013)	P.L. 113-277, Sec. 4 (Dec 2014)	OMB directive (Oct 2015)	P.L. 114-113, Division N, Title III (Dec 2015)
Skills gap assessments	No requirement.	DHS to, no later than one year after the assignment of cybersecurity codes and *annually until 2021,* identify cybersecurity areas of critical need in its workforce, including those that face acute and emerging skill shortages.	Agencies to identify the five cybersecurity specialty areas facing the largest talent gaps by December 31, 2015.	Agencies to, no later than one year after the assignment of cybersecurity codes and *annually until 2022*, identify cybersecurity areas of critical need in their workforces, including those that face acute and emerging skill shortages.
Oversight	OPM to *periodically monitor agencies' progress* in identifying and coding cybersecurity positions.	*DHS to submit* formal progress reports to Congress on (1) identifying and coding cybersecurity positions, and (2) identifying cybersecurity areas of critical need. GAO to submit a report to Congress on the status of their implementation of the law no later than three years after the date of enactment.	No requirement.	Agencies to submit *formal progress reports* to Congress on identifying and coding cybersecurity positions. *OPM to submit* a formal progress report on identifying cybersecurity areas of critical need. GAO to submit a report to Congress on the status of implementation of the law no later than three years after the date of enactment.

Source: CRS analysis of P.L. 113-277, P.L. 114-113, OPM Special Cybersecurity Workforce project documents, and OMB's Cybersecurity Strategy and Implementation Plan.

Selected Hiring and Pay Flexibilities Applicable to DOD and DHS Cybersecurity Positions

Congress has authorized hiring and pay flexibilities for DOD and DHS to enhance the recruitment and retention of cybersecurity professionals. OPM has also provided similar, but distinct, hiring flexibilities for certain DOD and DHS cybersecurity positions. The text box, below, provides a brief background on hiring and pay flexibilities.[45] The subsections below discuss

- selected hiring and pay flexibilities authorized by statute;
- selected OPM-issued hiring flexibilities;
- key functions of selected hiring and pay flexibilities; and
- an analysis of selected statutory provisions on hiring and pay flexibilities.

[45] This section does not discuss all hiring and pay flexibilities that can be used to fill federal cybersecurity positions. For a list of additional hiring and pay flexibilities applicable to federal cybersecurity positions, see OPM, memorandum from Mike Reinhold, Associate Director for Employee Services and Chief Human Capital Officer, "Cybersecurity Hiring, Pay, and Leave Flexibilities," November 23, 2015, at https://www.chcoc.gov/content/cybersecurity-hiring-pay-and-leave-flexibilities. The list does not include flexibilities that have been authorized by statute.

Hiring and Pay Flexibilities Defined

Hiring flexibilities – Hiring flexibilities generally exempt agencies from certain competitive hiring requirements in the federal hiring process and allow for tailored recruitment. Hiring flexibilities aim to reduce time-to-hire and may allow agencies to better recruit qualified individuals that best meet their needs. Examples of hiring flexibilities include direct-hire authority and excepted service appointment authorities.[46] Hiring flexibilities can be government-wide or agency-specific for one position or a group of positions. They can be issued by OPM or authorized by Congress.

Pay flexibilities – Pay flexibilities provide employees with additional compensation in order to enhance the recruitment and retention of top talent to the federal government. In general, pay flexibilities can either permanently increase or temporarily supplement an employee's base pay. They can also be performance or non-performance based. Examples of flexibilities that *increase* base pay include critical position pay authority and Quality Step Increases under the General Schedule (GS). Examples of flexibilities that *supplement* base pay include recruitment, relocation, and retention incentives and performance-based cash awards.[47] Similar to hiring flexibilities, pay flexibilities can apply to one position or a group of positions. Some pay flexibilities are issued by OPM, while others are authorized by Congress. Several OPM-issued pay flexibilities can be used at an agency's discretion, though some must be approved by OPM or OMB prior to use.

Selected Hiring and Pay Flexibilities Authorized by Statute

Congress enacted three laws that authorize hiring and pay flexibilities applicable to cybersecurity positions at DOD and DHS:

- P.L. 104-201, the National Defense Authorization Act for FY1997
- P.L. 113-277, the Border Patrol Pay Agent Reform Act of 2014
- P.L. 114-92, the National Defense Authorization Act for FY2016

The flexibilities were first established in P.L. 104-201 for DOD intelligence positions, although they have been used to fill positions that perform cybersecurity functions. For example, the Department of the Army used the flexibilities to fill a "Senior Intelligence Advisor, Cyber" position.[48] The hiring flexibilities authorized in P.L. 104-201 were used to justify establishing nearly identical flexibilities for cybersecurity positions at DOD and DHS. **Table 2**, below, briefly describes the coverage and legislative background of the three laws.

Table 2. Statutory Authorities Governing Selected Hiring and Pay Flexibilities Applicable to DOD and DHS Cybersecurity Positions

Feature	P.L. 104-201, Sec. 1632	P.L. 113-277, Sec. 3	P.L. 114-92, Sec. 1107
General authority	Authorizes the Secretary of Defense to (1) establish defense intelligence positions in the excepted service, and (2) fix the rates of pay for such positions.	Authorizes the Secretary of Homeland Security to (1) establish cybersecurity positions in the excepted service, and (2) fix the rates of pay for such positions.	Authorizes the Secretary of Defense to (1) establish positions at and in support of the U.S. Cyber Command in the excepted service, and (2) fix the rates of pay for such positions.

[46] For a list of certain hiring flexibilities, see OPM, *Human Resources Flexibilities and Authorities in the Federal Government*, August 2013, pp. 17-18, at https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/humanresourcesflexibilitiesauthorities.pdf.

[47] For a list of pay flexibilities, see ibid., pp. 41-47 and 56-57.

[48] The vacancy announcement is closed, but as of January 8, 2016, could still be viewed at https://www.usajobs.gov/GetJob/ViewDetails/420013200.

Feature	P.L. 104-201, Sec. 1632	P.L. 113-277, Sec. 3	P.L. 114-92, Sec. 1107
Coverage	DOD intelligence positions.	DHS cybersecurity positions.	DOD cybersecurity positions within and in support of the U.S. Cyber Command.
Enactment date	September 23, 1996	December 18, 2014	November 25, 2015
U.S. Code citation	10 U.S.C. §1601-1607	6 U.S.C. §147	N/A
Legislative background	First proposed in the Senate version of the NDAA for FY1995 (S. 1745, 104th Congress). Amended language from S. 1745 incorporated into P.L. 104-201.	First proposed in the DHS Cybersecurity Workforce Recruitment and Retention Act of 2014 (S. 2354, 113th Congress). Language from S. 2354 incorporated into P.L. 113-277.	First proposed in the Senate version of the NDAA for FY2016 (S. 1376, 114th Congress). Language from S. 1376 incorporated into P.L. 114-92.
References to flexibilities in P.L. 104-201	N/A	A Senate Committee on Homeland Security and Governmental Affairs report accompanying S. 2354 noted that flexibilities in P.L. 104-201 have enabled DOD to "build and maintain a strong cybersecurity workforce" and that similar flexibilities were "needed by DHS to address the ever-growing cyber threat to our national and economic security."	A Senate Committee on Armed Services report accompanying S. 1376 noted that the flexibilities proposed therein were modeled after the flexibilities in P.L. 104-201 and are "a very important factor in attracting and retaining the high caliber of personnel that are critical to the execution of the cyber warfare mission of the department [DOD]."

Source: CRS analysis of the laws cited in the table.

a. U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *DHS Cybersecurity Workforce Recruitment and Retention Act of 2014*, report to accompany S. 2354, 113th Cong., 2nd sess., S.Rept. 113-207 (Washington, DC: GPO, 2014), pp. 2-3.

b. U.S. Congress, Senate Committee on Armed Services, *National Defense Authorization Act for FY2016,* report to accompany S. 1376, 114th Cong., 1st sess., S.Rept. 114-49 (Washington, DC: GPO, 2015), pp. 219-220.

Selected OPM-Issued Hiring Flexibilities

OPM has also issued temporary hiring flexibilities for a limited number of cybersecurity positions at DOD and DHS.[49] The positions must require unique cybersecurity skills and knowledge that are explicitly specified in the flexibilities. The DOD flexibility must be used to fill positions within certain occupational series, while the DHS flexibility does not include such limitations. The DHS flexibility appears to be an interim recruiting solution for cybersecurity professionals until the regulations governing the hiring and pay flexibilities under P.L. 113-277 become effective. **Table 3**, below, summarizes key features of the flexibilities.

[49] OPM, "Excepted Service," 80 *Federal Register* 12045, March 5, 2015, at https://www.federalregister.gov/articles/2015/03/05/2015-05185/excepted-service; OPM, "Excepted Service," 80 *Federal Register* 69726, November 10, 2015, at https://www.federalregister.gov/articles/2015/11/10/2015-28566/excepted-service.

Table 3. OPM-Issued Hiring Flexibilities for Cybersecurity Positions

Feature	DOD Cybersecurity Positions	DHS Cybersecurity Positions
Number of positions	Up to 3,000.	Up to 1,000.
Coverage	Positions that require unique cybersecurity skills and knowledge to perform: (1) cyber risk and strategic analysis, (2) incident handling and malware/vulnerability analysis, (3) program management, (4) distributed control systems security, (5) cyber incident response, (6) cyber exercise facilitation and management, (7) cyber vulnerability detection and assessment, (8) network and systems engineering, (9) enterprise architecture, (10) investigation, (11) investigative analysis, and (12) cyber-related infrastructure inter-dependency analysis.	
Occupational series	**Department-wide**: Security (GS-0080), computer engineers (GS-0854), electronic engineers (GS-0855), computer scientists (GS-1550), operations research (GS-1515), criminal investigators (GS-1811), telecommunications (GS-0391), IT specialists (GS-2210). **U.S. Cyber Command**: Administrative and program series (GS-0301).	Not specified.
Applicable grades	GS-9 to GS-15	
Appointment type	Permanent, time-limited, or temporary.	Not specified.
Expiration date (date upon which hires must be completed)	December 31, 2015	June 30, 2016, or until the regulations governing hiring and pay flexibilities authorized under P.L. 113-277 become effective (whichever comes first).

Source: OPM, "Excepted Service," 80 *Federal Register* 12045, March 5, 2015, at https://www.federalregister.gov/articles/2015/03/05/2015-05185/excepted-service; OPM, "Excepted Service," 80 *Federal Register* 69726, November 10, 2015, at https://www.federalregister.gov/articles/2015/11/10/2015-28566/excepted-service.

Notes: The DHS authority also includes "intelligence analysis" as a required skill.

Key Functions of Hiring and Pay Flexibilities

The aforementioned hiring and pay flexibilities aim, respectively, to enhance the recruitment and retention of cybersecurity professionals at DOD and DHS by (1) designating cybersecurity positions as within the excepted service, and (2) allowing for additional compensation for cybersecurity professionals. The OPM-issued flexibilities do not explicitly authorize the use of the pay flexibilities.

Hiring Flexibilities: Excepted Service Designation

The hiring flexibilities described above allow covered DOD and DHS positions to be placed in the excepted service (see text box below for an explanation). As a result, DOD and DHS are *not* subject to the competitive hiring requirements in Title 5 of the *United States Code* that are placed on other agencies for covered positions. Rather, the authorized agencies can use alternative (and often agency-developed) recruitment, assessment, and selection methods for the positions that are sometimes seen as more flexible and efficient than regular competitive hiring procedures. These alternative hiring procedures are intended to allow for streamlined and tailored recruitment, which could expedite the hiring process. For example, DOD and DHS may waive public notice

requirements, including posting job announcements on USAJobs.gov, for covered positions.[50] This exception might allow the departments to reduce the number of applications to review and hire from a narrower group of individuals, thereby accelerating the hiring process.

The Excepted Service

The federal workforce includes the competitive service, excepted service, and Senior Executive Service. The *competitive service* includes the majority of executive branch positions, and includes positions that are open to all applicants and require a competitive process to acquire the position. The *Senior Executive Service (SES)* consists of executive management positions that oversee activities in approximately 75 agencies. The *excepted service* includes positions that are not in the competitive service or the SES.[51]

According to OPM, excepted service designations are provided "to fill special jobs or to fill any job in unusual or special circumstances," thereby enabling "agencies to hire when it is not feasible or not practical to use traditional competitive hiring procedures."[52] Individuals that meet an excepted service position's eligibility and minimum qualification requirements do not have to compete with other applicants. Excepted service designations can be issued by OPM or authorized by Congress. Flexibilities authorized by statute are distinct from OPM-issued flexibilities and can be implemented without OPM approval. Their structure and functions might differ.

Pay Flexibilities: Additional Compensation

The laws described above provide DOD and DHS with the opportunity to offer cybersecurity professionals additional compensation that is not typically available to all federal employees. The flexibilities seek to increase DOD's and DHS's abilities to compete for top cybersecurity talent. A report accompanying the DHS Cybersecurity Workforce Recruitment and Retention Act of 2014, for example, asserted that the pay flexibilities for DOD intelligence positions provide DOD with "significant latitude in setting pay and benefits [for cybersecurity positions], adding on regional or other adjustments to pay, and offering further specific financial incentives."[53]

Fixed Rates of Pay

The laws for DOD and DHS authorize the departments to fix salaries for positions covered under their respective workforce flexibilities at rates of comparable DOD positions and fill such positions without regard to the classification and compensation requirements in any other law.[54] Using these flexibilities, the departments can establish alternative pay systems outside of the GS system and develop their own criteria for setting and adjusting salaries for positions within that system.[55] According to a 2011 GAO report on the federal cybersecurity workforce, characteristics of certain non-GS systems can allow agencies to offer employees higher salaries compared to

[50] Public notice requirements specified in 5 U.S.C. §3327, 5 U.S.C. §3330, and 5 C.F.R. Part 330, Subpart A only apply to competitive service positions.

[51] 5 U.S.C. §2103; OPM, "Hiring Authorities, Competitive Hiring, Overview," at http://www.opm.gov/policy-data-oversight/hiring-authorities/competitive-hiring/#url=Overview; and OPM, "Hiring Authorities, Excepted Service," at http://www.opm.gov/policy-data-oversight/hiring-authorities/excepted-service/.

[52] OPM, "Hiring Authorities, Excepted Service"; 5 C.F.R. Part 213.

[53] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *DHS Cybersecurity Workforce Recruitment and Retention Act of 2014*, report to accompany S. 2354, 113th Cong., 2nd sess., S.Rept. 113-207 (Washington, DC: GPO, 2014), p. 2.

[54] 10 U.S.C. §1601(b); 10 U.S.C. §1602(a); 6 U.S.C. §147(b)(2)(A); 6 U.S.C. §147(b)(1)(B); P.L. 114-92, sec.1107.

[55] Use of alternative personnel systems can be authorized by OPM or Congress. For more information on alternative personnel systems authorized by OPM, see OPM, "Alternative Personnel Systems, About APS," at http://archive.opm.gov/aps/about/index.aspx; and OPM, "Alternative Personnel Systems, Frequently Asked Questions," at http://archive.opm.gov/aps/about/faq/index.aspx.

their GS system-bound counterparts.[56] As stated earlier, agencies have argued that non-GS systems can increase an agency's ability to attract and retain cybersecurity professionals.[57]

Additional Monetary Incentives

Individuals filling DOD and DHS cybersecurity positions through the flexibilities authorized by statute are eligible for additional monetary incentives.[58] These incentives can include one-time cash payments or base pay increases and can be performance or non-performance based. In many cases, these incentives can be given to all federal employees.[59] For example, regarding non-performance-based flexibilities, all agencies have the discretion to provide recruitment incentives for positions that would be difficult to fill in the absence of such an incentive.[60] Agencies also have the discretion to provide performance-based cash awards to employees for work that "contributes to the efficiency, economy, or other improvement of government operations."[61]

Some monetary incentives authorized under the DOD and DHS laws, however, are only available to employees covered under the laws and can allow these employees—including cybersecurity professionals—to earn higher base salaries (exclusive of locality-pay adjustments) than their GS counterparts. For example, cybersecurity employees covered under the Defense Civilian Intelligence Personnel System (DCIPS) can receive awards that cause their base salaries to exceed the maximum pay rate of their position's grade, while GS employees cannot (the text box below provides an example). DCIPS[62] is a DOD-specific, alternative personnel management system that encompasses DOD intelligence positions covered under P.L. 104-201 and includes a General Grade (GG) salary structure that aligns with the GS system's 15-grade structure.[63]

Higher Salaries for Cybersecurity Employees: GS and DCIPS

The scenarios below demonstrate how awards that increase base pay can allow cybersecurity employees covered under DCIPS to earn higher annual salaries compared to their GS counterparts. For the purposes of these scenarios, a base pay increase is defined as a two-step increase within a position's grade (e.g., GS-7, Step 1 to GS-7, Step 3).

GS: A federal employee is currently in a GS-15, Step 10 position—the maximum step of the highest grade. The employee receives the highest possible performance rating ("outstanding" or equivalent). The employee is *not* eligible for a two-step base pay increase within a GS grade, as the employee's base salary cannot exceed the maximum step of the GS-15 grade.[64] The employee's salary remains at the GS-15, step 10 level.[65] If the employee does not receive a cash award (i.e., bonus), the performance level achieved may not be recognized.

[56] For a list of these characteristics, see Table 7 in GAO, *Cybersecurity Human Capital, Initiatives Need Better Planning and Coordination*, GAO-12-8, November 29, 2011, p. 30.

[57] Ibid., pp. 29-31.

[58] 10 U.S.C. §1603; 6 U.S.C. §147(b)(3); P.L. 114-92, sec. 1107. The incentives cannot exceed the amounts authorized for comparable Title 5 positions.

[59] For more information on monetary incentives that can be accessed by all agencies, see OPM, *Human Resources Flexibilities and Authorities in the Federal Government*, August 2013, pp. 41-47 and 56-57.

[60] Ibid., p. 41; 5 U.S.C. §5753; 5 C.F.R. Part 575, Subpart A.

[61] OPM, *Human Resources Flexibilities and Authorities in the Federal Government*, August 2013, p. 56; 5 U.S.C. §4503; 5 C.F.R. §451.104(a)(1).

[62] For more information on DCIPS, see DOD, "Defense Civilian Personnel Intelligence System," at http://dcips.dtic.mil/.

[63] DOD, "Department of Defense Civilian Intelligence Personnel System (DCIPS) GG Grade Ranges for 2016, PDF p. 1, at http://dcips.dtic.mil/documents/DCIPS_Pay_Rates-2016.pdf.

[64] A two-step base-pay increase within a GS grade is known as a Quality Step Increase (QSI). Employees at the top of their grade level (step 10) are not eligible for QSIs. For more information on QSIs, see 5 U.S.C. §5336, 5 C.F.R. Part 531, Subpart E; and OPM, "Fact Sheet, Quality Step Increase," at https://www.opm.gov/policy-data-oversight/pay-(continued...)

DCIPS: A federal employee is currently in a GG-15, Step 10 position—the maximum step of the highest grade.[66] The employee has been in the GG-15 grade for at least three consecutive performance periods and has received the highest possible performance rating ("outstanding," or a performance rating that places the employee in the top 10% among his or her peers for those three periods). The employee *is* eligible for a two-step base-pay increase within the GG-15 grade, as DCIPS allows employees to exceed the maximum step of the GG-15 grade upon receiving a performance award.[67] The employee's base salary increases to a level that exceeds the GS-15, Step 10 base maximum.[68]

Analysis of Selected Statutory Provisions for Hiring and Pay Flexibilities

This section includes an analysis of selected provisions from the three laws authorizing hiring and pay flexibilities for DOD intelligence positions (P.L. 104-201), DHS cybersecurity positions (P.L. 113-277), and DOD cybersecurity positions affiliated with the U.S. Cyber Command (P.L. 114-92). The analysis highlights key structural differences between the selected provisions. **Appendix A** includes a side-by-side analysis of key provisions in each of the laws.

Probationary Period

New employees hired into DOD or DHS cybersecurity positions are subject to a three-year probationary period.[69] While no similar extended probationary period is statutorily required for DOD intelligence personnel, DOD has instituted a two-year "trial period" for many of these positions.[70] In addition, existing DOD and DHS cybersecurity employees that are scheduled to be converted to the excepted service have the right to refuse moving to the excepted service. The law governing DOD intelligence positions contains no similar language. Employees in the excepted service cannot apply for career and career-conditional federal jobs (i.e., jobs that are not open to all U.S. citizens) and therefore might be less inclined to accept the conversion.[71]

(...continued)

leave/pay-administration/fact-sheets/quality-step-increase/.

[65] The GS-15, Step 10 salary rates vary by locality. For a list of 2016 GS pay rates, see OPM, "2016 General Schedule (GS) Locality Pay Tables," at https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2016/general-schedule/.

[66] DOD, "Defense Civilian Intelligence Personnel System (DCIPS) GG Grade Ranges for 2016," January 10, 2016, PDF p. 1.

[67] A two-step base-pay increase within a DCIPS grade is known as a Sustained Quality Increase (SQI). Unlike the GS, employees at the top of their grade level (step 10) are eligible for SQIs. For more information on SQIs, see DOD, "DOD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Awards and Recognition, DOD Instruction Number 1400.25, Volume 2008, October 4, 2015, pp. 9-11, at http://www.dtic.mil/whs/directives/corres/pdf/140025_vol2008.pdf.

[68] See, for example: OPM, "Salary Table 2016-GS," at https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2016/GS.pdf; DOD, "Defense Civilian Intelligence Personnel System (DCIPS) GG Grade Ranges for 2016," January 10, 2016, PDF p. 1.

[69] The standard probationary period for a new federal employee in a competitive service position is one year. See 5 C.F.R. §315.801 and 5 .C.F.R. §315.802.

[70] DOD, "DOD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Awards and Recognition, DOD Instruction Number 1400.25, Volume 2008, October 4, 2015, pp. 13-14. The DCIPS trial period is similar to the federal probationary period, during which an employee can be removed at will.

[71] For more information on career and career-conditional employment, see 5 C.F.R. Part 315, Subpart B.

Implementation Plan

The laws for DOD and DHS cybersecurity positions require an implementation plan describing how the hiring and pay flexibilities will be used, while the law for DOD intelligence positions does not. The content and submission requirements, however, differ between plans. P.L. 114-92 requires DOD to submit an implementation plan to Congress prior to using the flexibilities. The flexibilities will only become effective 30 days after Congress receives the plan. In addition, the plan's content must include "(1) an assessment of the scope of positions covered by the flexibilities, (2) a plan for using the flexibilities, and (3) an assessment of the anticipated workforce needs of the U.S. Cyber Command across the future-years' defense plan."[72] P.L. 113-277, in contrast, does not require DHS to include specific information in the implementation plan, nor does it preclude DHS from using the flexibilities therein prior to submitting the plan.

Reporting Requirements

DOD and DHS are required to report annually on the use of hiring and pay flexibilities for covered cybersecurity positions. The reports' content requirements are identical and must include recruitment and retention data—such as the number of hires, separations, and retirements for covered cybersecurity positions—among other things.[73] The report authors and submission timelines, however, differ. P.L. 113-277 directs DHS to develop the annual report, while P.L. 114-92 requires OPM, in coordination with DOD, to develop the report. Further, the plan for DHS flexibilities must be submitted annually for four years after the date of enactment, compared to annually for five years after the date of enactment under the plan for DOD flexibilities. The law for DOD intelligence positions does not contain any reporting requirements.

Congressional Oversight Issues

Congress has shown an interest in ensuring that the federal cybersecurity workforce is defined and identified.[74] Congress has also shown an interest in ensuring that hiring and pay flexibilities for cybersecurity positions at DOD and DHS are properly implemented and achieve their intended purposes.[75] If such interest continues, Congress could enhance its oversight of these efforts to increase its awareness and knowledge of their implementation. The subsections below discuss potential issues in the absence of enhanced congressional oversight related to (1) identifying and defining the federal cybersecurity workforce, and (2) hiring and pay flexibilities that can be used to fill DOD and DHS cybersecurity positions.

Identifying and Defining the Federal Cybersecurity Workforce

Efforts to define and identify federal cybersecurity workforce positions have largely been undertaken by OPM. OPM, however, is not currently required to report on its progress in identifying and coding all federal cybersecurity positions to Congress, nor has it released its cybersecurity dataset or a government-wide count of the cybersecurity workforce to Congress. Further, OMB's CSIP does not require agencies to report identified skills gaps in their cybersecurity workforces to Congress. Congressional knowledge of the progress of these

[72] P.L. 114-92, sec. 1107.

[73] A comprehensive list of these content requirements can be found in **Appendix B**.

[74] See, for example, P.L. 114-113, Division N, Title III.

[75] See, for example, P.L. 113-277, sec. 3, and P.L. 114-92, sec. 1107.

evolving efforts, therefore, might be limited or incomplete, which might make it difficult for Congress to (1) identify potential conflicting efforts between OMB, OPM, and Congress in assessing the capabilities of the federal cybersecurity workforce, and (2) gauge the utility of hiring and pay flexibilities for cybersecurity positions.

Potential Conflicting Efforts to Assess the Federal Cybersecurity Workforce

The lack of a requirement for progress reports may make it difficult for Congress to identify or prevent potentially conflicting efforts to identify cybersecurity workforce gaps between existing laws and OMB/OPM directives. For example, as stated previously, the CSIP required all agencies to identify their top five cyber talent gaps, and P.L. 113-277 and P.L. 114-113 require DHS and executive branch agencies to identify cybersecurity specialty areas of critical need—including those facing acute and emerging skill shortages.[76] OPM issued guidance to help agencies identify their top five cyber talent gaps.[77] OPM is also required under P.L. 113-277 and P.L. 114-92 to issue separate guidance to help DHS and executive branch agencies identify cybersecurity areas of critical need. If OPM's guidance for identifying cyber talent gaps differs substantially from its guidance for identifying cybersecurity areas facing acute or emerging skill shortages, it could result in different positions identified as facing workforce gaps. This might affect agencies' ability to address staffing needs.

Utility of Hiring and Pay Flexibilities

Congress's knowledge of agencies' cybersecurity workforce capabilities and needs might be affected by lack of access to OPM's dataset and lack of formal notification about cybersecurity skills gaps identified through the CSIP. Consequently, it might be difficult for Congress to definitively determine the need for or the proper structure of hiring and pay flexibilities to address those needs. This could lead to the absence of certain hiring and pay flexibilities, authorization of new flexibilities that are not necessarily needed, or the realization that existing flexibilities do apply to the specific agency components. For instance, suppose a federal department identifies cybersecurity skills gaps in one of its major components without a full and accurate count of its workforce and Congress subsequently authorizes hiring and pay flexibilities to fill those positions. If the agency, after accurately measuring the size and composition of its workforce, determines that a different component faces skills gaps, the existing flexibilities would not help to address such gaps.

Issues Related to Hiring and Pay Flexibilities for DOD and DHS Cybersecurity Positions

The laws governing flexibilities for DOD and DHS cybersecurity positions require the departments to report to Congress on their use, while neither the law for DOD intelligence positions nor the OPM-issued flexibilities do. Further, existing reporting requirements for the flexibilities do not require the departments to identify challenges to using the flexibilities or to measure their effectiveness. DOD and DHS have broad discretion to determine the structure and implementation of statutorily authorized hiring and pay flexibilities, such as what positions the

[76] It is unclear if the terms "acute and emerging skills shortages" and "cyber talent gaps" refer to different concepts.

[77] OPM, memorandum from Mark Reinhold, Associate Director of Employee Services, to Chief Human Capital Officers and Chief Information Officers, "Guidance for Identifying Top Five Cyber Talent Gaps," November 23, 2015, at https://www.chcoc.gov/content/guidance-identifying-top-five-cyber-talent-gaps. The resource charts are on OMB's MAX website and are only accessible by executive branch agency staff.

flexibilities apply to and how they are to be used. This discretion can create the potential for discrepancies between the intended and actual use of the flexibilities. Were Congress to be interested in identifying and addressing any potential discrepancies, as well as gauging the flexibilities' effectiveness in improving the recruitment and retention of cybersecurity professionals at DOD and DHS, it might need to enhance its oversight by clarifying reporting requirements.

The subsections below discuss issues related to (1) usage data and its potential impact, (2) effectiveness measurement, and (3) training with regard to the DOD and DHS hiring and pay flexibilities.

Lack of Data on Use of Certain Cybersecurity Hiring Flexibilities at DOD and DHS

The law for DOD intelligence positions, and the OPM-issued hiring flexibilities for certain DOD and DHS cybersecurity positions, do not require the departments to report, among other things, (1) the total number of employees hired using the flexibilities,[78] (2) the specific types of positions filled through the flexibilities, or (3) in which components the positions are located. A lack of data on the use of hiring and pay flexibilities could reduce Congress's ability to determine how much they are used and to what effect.

Appropriate Use of Flexibilities

In the absence of data on use of the flexibilities issued by OPM or authorized under the law for DOD intelligence positions, Congress might find it difficult to ensure that these flexibilities are being used to fill appropriate positions. For example, at least one cybersecurity workforce expert expressed concern that DHS may have used a past OPM-issued cybersecurity hiring flexibility to fill non-cybersecurity positions.[79]

Maximized Use of Flexibilities

The absence of data may make it difficult for Congress to determine to what extent the flexibilities are used, and what challenges may inhibit their maximum use. Ultimately, this could affect future decisions regarding the authorization of additional flexibilities or changes to the structure of existing flexibilities. For example, suppose that DHS uses the OPM-issued hiring flexibility to fill 200 cybersecurity positions—20% of the maximum allowed by the flexibility (up to 1,000 positions). If DHS had no additional positions to fill, additional flexibilities might not be needed. If DHS encountered implementation challenges that prevented further use of the flexibility, however, structural changes to the flexibility may be needed. Similarly, suppose that DHS does not use the pay flexibilities authorized under P.L. 113-277. While the lack of use could indicate that the flexibilities are not needed, it may also stem from budget constraints.

[78] Section 301 of the House-passed version of the National Cybersecurity and Critical Infrastructure Protection Act of 2014 (H.R. 3696, 113th Congress) included a provision that would have required DHS to report the total number of individuals hired under a past OPM-issued cybersecurity hiring flexibility, suggesting that such data are not readily available to Congress.

[79] In May 2014, Alan Paller, an expert on the federal cybersecurity workforce and one of the authors of DHS's Cybersecurity Task Force Report, wrote in the SANS.org newsletter that "DHS IT managers hijacked [the hiring authority] to hire people, without cyber skills, for regular IT roles, bypassing normal hiring rules." See SANS, "Newsletters: Newsbites," Volume XVI – Issue #39, at http://www.sans.org/newsletters/newsbites/xvi/39. SANS is "a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world." See SANS, "About," at http://www.sans.org/about/.

Utility of Flexibilities for the U.S. Cyber Command

A lack of data on how frequently the flexibilities for DOD intelligence positions are being used to fill positions affiliated with the U.S. Cyber Command may make it difficult for Congress to gauge the utility of new flexibilities authorized for Command positions under P.L. 114-92. It appears that some positions affiliated with the Command are being filled using the existing flexibilities for DOD intelligence positions. The Departments of the Army and Navy, for example, are using the flexibilities to fill cybersecurity positions in units that support the Command.[80] The flexibilities, therefore, might not be needed as much or used as often as envisioned if a sizeable portion of covered positions can be filled using existing flexibilities.

Effectiveness of Hiring and Pay Flexibilities

Existing reporting requirements for the hiring and pay flexibilities measure the *use* of hiring and pay flexibilities, but do not necessarily measure their *effectiveness*. For example, the law for DHS cybersecurity positions requires the department to detail how it plans to recruit and retain employees in cybersecurity positions and how it will measure progress in doing so. The laws do not, however, task DHS and DOD with determining whether and in what ways specific aspects of the hiring and pay flexibilities improved the departments' ability to attract and retain qualified cybersecurity professionals, or whether these professionals have improved the quality and capacity of the departments' cybersecurity workforces.

Training on Structure and Use of Flexibilities

The laws governing flexibilities for DOD intelligence, DHS cybersecurity, and DOD cybersecurity positions at the U.S. Cyber Command do not include provisions to require human resources staff (including component-level hiring managers and department-level staff in the Office of the Chief Human Capital Officer) to receive training on the availability, structure, and operation of cybersecurity hiring and pay flexibilities. Rather, P.L. 113-277 and P.L. 114-92 require DOD and DHS to *describe* the training provided to *supervisors using the flexibilities* in the aforementioned annual reports to Congress.

A lack of staff training might impact effective use of the flexibilities. Untrained hiring managers and human resources staff might not know about the flexibilities, the positions they apply to, how to properly implement them, and the positions for which they are most appropriate. For example, as mentioned earlier, it appears that certain cybersecurity positions affiliated with the U.S. Cyber Command could be filled under the flexibilities authorized under P.L. 104-201 or P.L. 114-92.

Oversight Policy Options

Pursuant to its oversight authority, Congress could consider several oversight policy options to enhance its knowledge and awareness of identification and recruitment efforts for the federal cybersecurity workforce. Seven options are presented in this section, though other policy options exist. The first two policy options relate to monitoring OPM and OMB initiatives to define and identify federal cybersecurity positions. The remaining five options relate to monitoring the

[80] The vacancy announcements are closed, but as of January 8, 2016, could still be viewed at: https://www.usajobs.gov/GetJob/ViewDetails/423794200 and https://www.usajobs.gov/GetJob/ViewDetails/417782000. The announcements are for vacancies in the U.S. Army Intelligence and Security Command and U.S. Cyber Fleet Command, which support the U.S. Cyber Command.

implementation of hiring and pay flexibilities used to fill DOD and DHS cybersecurity positions. CRS takes no position on the advisability of these and other potential policy options.

This section does not present broader policy options that address the capabilities of the federal cybersecurity workforce, such as the establishment of additional hiring and pay flexibilities, other personnel tools that could be used to recruit and retain cybersecurity professionals, and whether federal cybersecurity professionals are enabling agencies to fulfill their respective missions.

1. Notification of Progress on OPM Cybersecurity Dataset

OPM could be required to notify appropriate congressional committees on the status of the cybersecurity dataset, including when the dataset is completed and released to the public on OPM's online workforce data portal. In exercising its oversight authority, Congress may require these notifications to occur annually, semi-annually, quarterly, or on any other standard timeline. OPM could also be required to brief appropriate congressional committees on the structure and functions of the dataset upon its release. This could include (but not be limited to) the data it presents, how the data can be used to generate a government-wide count of the cybersecurity workforce, how it will be kept up to date, and anticipated enhancements and adjustments to be made.

2. GAO Evaluation of OPM Cybersecurity Dataset

As mentioned previously, P.L. 113-277 and P.L. 114-113 require GAO to submit a report to Congress describing the status of identifying, coding, and evaluating critical needs of cybersecurity positions at DHS and executive branch agencies. The laws do not, however, explicitly require GAO to evaluate OPM's dataset. In its oversight capacity, Congress could additionally direct GAO to study the operation and effectiveness of the OPM cybersecurity dataset one year after it becomes operational. The study could evaluate, whether the dataset and OPM cybersecurity data codes accomplish the goals listed below. The study could also evaluate the validity of reported skills gaps in agencies' cybersecurity positions.

> (1) identify positions for which the primary function is cybersecurity;
>
> (2) enable OPM and agencies to determine the baseline capabilities of the workforce, examine hiring trends, identify skills gaps, and more effectively recruit, hire, train, develop, and retain an effective cybersecurity workforce;
>
> (3) allow HR professionals to better understand the workforce and what issues need to be addressed; and
>
> (4) provide a platform for organizations outside of the federal government to similarly organize their cybersecurity professionals.[81]

3. Conform Reporting Requirements for DOD and DHS Flexibilities

Congress could amend existing statues to extend the reporting requirements articulated in the law for DHS cybersecurity positions—or the law for DOD cybersecurity positions—to DOD

[81] OPM, "The Use and Usefulness of the Cybersecurity Data Element," December 6, 2012, PDF p. 4. These are the intended goals of the OPM cybersecurity data codes, which align with the goals for OPM's cybersecurity dataset initiative.

intelligence positions. Congress could also add a new reporting provision that requires DOD and DHS to provide information on any challenges encountered in implementing the flexibilities under P.L. 104-201, P.L. 114-92, and P.L. 113-277. Reporting requirements enhance congressional oversight of the hiring and pay flexibilities used for DOD intelligence positions. In addition, the reporting requirements might allow Congress to compare the use of the DOD and DHS hiring and pay flexibilities.

4. Additional Data on DOD Flexibilities

Congress could include the metrics listed below in the annual reporting requirements for DOD intelligence positions (P.L. 104-201) and DOD positions affiliated with the U.S. Cyber Command (P.L. 114-92). The metrics could provide Congress with greater clarity on the extent to which the flexibilities under the laws are being used to fill cybersecurity positions. Such clarity might better position Congress to determine the utility of the flexibilities and the need (or lack thereof) for additional flexibilities for DOD cybersecurity positions.

For DOD intelligence positions (P.L. 104-201):

1. Total number of covered cybersecurity positions filled using the hiring flexibilities authorized by P.L. 104-201.
2. Total number of covered cybersecurity positions filled using *other* hiring flexibilities.
3. Percentage of filled cybersecurity positions that are affiliated with the U.S. Cyber Command.

For DOD positions affiliated with the U.S. Cyber Command (P.L. 114-49):

1. Total number of covered cybersecurity positions filled using the hiring flexibilities authorized by P.L. 114-49.
2. Total number of covered positions filled using *other* hiring flexibilities.
3. Percentage of covered positions filled through other existing hiring flexibilities.

5. Additional Data on OPM-Issued Flexibilities

DOD and DHS could be required to report their use of OPM-issued hiring flexibilities for cybersecurity positions. The requirements could include, (1) the number of positions filled using the flexibility; (2) the pay plan, occupation, series, and grade of the position; (3) the nature of action of each hire; and (4) any challenges encountered in implementing the flexibilities. Such data might enhance Congress's capacity to determine the extent to which these flexibilities are being, or have been used—and any barriers to maximizing their use. This information could, in turn, assist Congress in addressing any barriers to using statutorily authorized flexibilities and determining the utility of additional flexibilities.

6. Training for DOD and DHS Staff on Flexibilities

DOD and DHS could be required to provide training on the proper use and implementation of the hiring and pay flexibilities for cybersecurity positions to hiring managers and human resources staff listed below.[82] Congress could require the training to include a review of the existing

[82] These training requirements could apply to contractors fulfilling the positions listed below.

authorities that can be applied to cybersecurity positions. Training might allow staff to better understand when and how to use the flexibilities.

1. **Department-level human resources (HR) staff that manage the civilian workforce**

   This could include staff within the Office of Chief Human Capital Officer (CHCO), as well as other HR units that might be involved in civilian workforce issues.

2. **Department and component-level staff that develop implementing guidance for hiring and pay flexibilities**

   DHS and DOD often issue implementing guidance for hiring and pay flexibilities at the department and component levels. It might be useful for staff charged with issuing implementing guidance to receive training on the structure and functions of the flexibilities.

3. **Component-level supervisors and hiring managers that use, or would use, the flexibilities**

   DHS and DOD supervisors and hiring managers that use, or would use, the flexibilities might also benefit from training.

7. Report on the Effectiveness of Hiring and Pay Flexibilities

The Inspectors General at DOD and DHS could be required to report on how effective the hiring and pay flexibilities authorized through statute—and the specific features—have been in recruiting and retaining qualified cybersecurity professionals. For example, the reports could include an analysis of whether the hiring flexibilities reduced time to hire, and whether the reduced time to hire attracted qualified cybersecurity professionals to the departments,[83] whether monetary incentives were a primary factor in attracting and retaining cybersecurity professionals to the federal government, which types of monetary incentives were most effective in doing so (e.g., performance awards or student loan repayments), and potentially other related matters.

[83] For the purposes of this report, time to hire is defined as the total number of days between an applicant job interview and a conditional job offer.

Appendix A. Side-by-Side Analysis of Selected Provisions from Statutory Authorities for DOD Intelligence, DHS Cybersecurity, and DOD Positions at the U.S. Cyber Command

Provision	DOD Intelligence (P.L. 104-201, sec. 1632)	DHS Cybersecurity (P.L. 113-277, sec. 3)	DOD Cyber Command (P.L. 114-92, sec. 1107)
Title	Management of Civilian Intelligence Personnel	Cybersecurity Recruitment and Retention	U.S. Cyber Command Recruitment and Retention
Date of enactment	September 23, 1996	December 18, 2014	November 25, 2015
General authority	Authorizes the Secretary of Defense to (1) establish defense intelligence positions in the excepted service, including those identified as Defense Intelligence Senior Level and Defense Intelligence Senior Executive Service positions established under 10 U.S.C. §1606-1607; and (2) appoint qualified individuals to such positions.	Authorizes the Secretary of Homeland Security to (1) establish cybersecurity positions in the excepted service, including those formerly identified as Senior Executive Service (SES) or Senior Level (SL); and (2) appoint qualified individuals to such positions.	Authorizes the Secretary of Defense to (1) establish positions at and in support of the U.S. Cyber Command in the excepted service, and (2) appoint qualified individuals to such positions.
Covered positions	Civilian intelligence positions as an intelligence officer or intelligence employee of a DOD intelligence component.	Positions in which individuals perform, manage, or supervise cybersecurity responsibilities.	Positions within the U.S. Cyber Command, elements of the Command enterprise relating to cyberspace operations, and military branch elements supporting the Command.
Removal of certain legal hiring requirements	Authorizes respective Secretaries to fill covered positions without regard to appointment, number, classification, and compensation requirements in any other law.		
Rates of basic pay	Allows the Secretary to fix rates of basic pay for covered positions to rates of comparable DOD positions. Maximum pay cannot exceed "established for DOD employees by law or regulation."	Allows the Secretary to fix rates of basic pay for covered positions to rates for comparable positions in DOD. Maximum pay rates are subject to the same limitations imposed on comparable DOD positions.	Allows the Secretary to fix rates of basic pay for covered positions to rates for comparable positions in DOD (i.e., those that perform, manage, or supervise functions that execute DOD's cyber mission). Maximum pay rates are subject to the same limitations imposed on comparable DOD positions.
Prevailing rates of pay	Allows respective Secretaries to, pursuant to 5 U.S.C §5341, fix rates of pay for individuals in a recognized trade or craft according to their prevailing rates under the Federal Wage System.		
Additional compensation	Allows respective Secretaries to provide employees in covered positions with monetary benefits, incentives, and allowances that do not exceed amounts for comparable Title 5 positions.		

Provision	DOD Intelligence (P.L. 104-201, sec. 1632)	DHS Cybersecurity (P.L. 113-277, sec. 3)	DOD Cyber Command (P.L. 114-92, sec. 1107)
Probationary period	No similar provisions.	Requires a three-year probationary period for covered positions.	
Conversion to excepted service	No similar provisions.	Employees in competitive service positions that will be converted to the excepted service may refuse the conversion.	
Implementation plan	No similar provisions.	Requires the Secretary to submit a plan detailing use of the authorities no later than 120 days after enactment to the following committees: (1) Senate Committee on Homeland Security and Governmental Affairs, (2) Senate Committee on Appropriations, (3) House Committee on Homeland Security, and (4) the House Committee on Appropriations.	Requires the Secretary to submit an implementation plan for the authority to the congressional defense committees. The authority would go into effect 30 days after submission of the plan. The plan must include information on the plan for using the authority, positions covered, and anticipated workforce needs for the U.S. Cyber Command.
Required regulations	No requirement to promulgate regulations. Requires the Secretary to submit any prescribed regulations to Congress 60 days before they become effective.	Requires each Secretary, in coordination with Director of OPM, to promulgate regulations to administer the authority.	
Reporting requirements	No similar provisions.	Requires the Secretary to, every year for four years after enactment, submit an annual report detailing the use of the authority to the (1) Senate Committee on Homeland Security and Governmental Affairs, (2) Senate Committee on Appropriations, (3) House Committee on Homeland Security, and (4) the House Committee on Appropriations.	Requires the Secretary to, every year for five years after enactment, submit an annual report detailing the use of the authority to the (1) Senate Committee on Armed Services, (2) Senate Committee on Homeland Security and Government Affairs, (3) Senate Committee on Appropriations, (4) House Committee on Armed Services, (5) House Committee on Oversight and Government Reform, and (6) House Committee on Appropriations.

Source: CRS analysis of the laws cited.

Notes: The table does not include all provisions included in laws cited.

Appendix B. Reporting Requirements

P.L. 113-277, sec. 3	P.L. 114-92, sec. 1107
"(c) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this section, and every year thereafter for 4 years, the Secretary shall submit to the appropriate committees of Congress a detailed report that—	"(g) ANNUAL REPORT.—(1) Not later than one year after the date of the enactment of this section and not less frequently than once each year thereafter until the date that is five years after the date of the enactment of this section, the Director of the Office of Personnel Management, in coordination with the Secretary, shall submit to the appropriate committees of Congress a detailed report on the administration of this section during the most recent one-year period.
"(1) discusses the process used by the Secretary in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by an individual for a qualified position;	"(2) Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:
"(2) describes—	"(A) A discussion of the process used in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by an individual for a qualified position.
"(A) how the Secretary plans to fulfill the critical need of the Department to recruit and retain employees in qualified positions;	"(B) A description of the following:
"(B) the measures that will be used to measure progress; and	"(i) How the Secretary plans to fulfill the critical need of the Department to recruit and retain employees in qualified positions.
"(C) any actions taken during the reporting period to fulfill such critical need;	"(ii) The measures that will be used to measure progress.
"(3) discusses how the planning and actions taken under paragraph (2) are integrated into the strategic workforce planning of the Department;	"(iii) Any actions taken during the reporting period to fulfill such critical need.
"(4) provides metrics on actions occurring during the reporting period, including—	"(C) A discussion of how the planning and actions taken under subparagraph (B) are integrated into the strategic workforce planning of the Department.
"(A) the number of employees in qualified positions hired by occupation and grade and level or pay band;	"(D) The metrics on actions occurring during the reporting period, including the following:
"(B) the placement of employees in qualified positions by directorate and office within the Department;	"(i) The number of employees in qualified positions hired, disaggregated by occupation, grade, and level or pay band.
"(C) the total number of veterans hired;	"(ii) The placement of employees in qualified positions, disaggregated by military department, Defense Agency, or other component within the Department.
"(D) the number of separations of employees in qualified positions by occupation and grade and level or pay band;	"(iii) The total number of veterans hired.
"(E) the number of retirements of employees in qualified positions by occupation and grade and level or pay band; and	"(iv) The number of separations of employees in qualified positions, disaggregated by occupation and grade and level or pay band.
"(F) the number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions by occupation and grade and level or pay band;	"(v) The number of retirements of employees in qualified positions, disaggregated by occupation, grade, and level or pay band.
"(5) describes the training provided to supervisors of employees in qualified positions at the Department on the use of the new authorities.	"(vi) The number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions, disaggregated by occupation, grade, and level or pay band.
	"(E) A description of the training provided to supervisors of employees in qualified positions at the Department on the use of the new authorities.

Source: P.L. 113-277 and P.L. 114-92.

Author Contact Information

(name redacted)
Analyst in Government Organization and Management
[redacted]@crs.loc.gov, 7-....

(name redacted)
Analyst in American National Government
[redacted]@crs.loc.gov , 7-....