U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES' RESPONSE TO:

NATIONAL INSTITUTE OF SCIENCE AND STANDARDS' (NIST) REQUEST FOR INFORMATION (RFI)

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE: WORKFORCE DEVELOPMENT

DOCUMENT CITATION: 82 FR 32172
DOCKET NUMBER: 170627596-7596-01
DOCUMENT NUMBER: 2017-14553

IN ACCORDANCE WITH:

EXECUTIVE ORDER 13800, "STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE"

Due August 2, 2017

TABLE OF CONTENTS

GENERAL INFORMATION

QUESTION 1

Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? Note: Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (e.g., personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.

CYBERSECURITY WORKFORCE EDUCATION AND TRAINING AT HHS

The Department of Health and Human Services (HHS) is not a cybersecurity academic or training institute, and it is not a cybersecurity educator. HHS exists to protect the health and wellbeing of all Americans. The Department holds 1-in-3 Americans' personally identifiable information. We respond to disease outbreaks, such as Zika; we achieve medical breakthroughs such as cracking the genome and precision medicine; and we provide medical and human services to our citizens. None of this would be possible without our vast and secure applications, systems, and information technology (IT) networks. While cybersecurity education is not its primary mission, HHS is setting the standard for IT and cybersecurity that promotes people's health and welfare, protects clinical drug trials that improve people's lives, and ensures our children and elderly are getting the secure services they need.

The HHS Office of the Chief Information Officer (OCIO) and Office of Human Resources (OHR) have, therefore, partnered to comprehensively address IT and cybersecurity workforce business needs and legislative requirements while improving our ability to attract, develop, and retain world-class cybersecurity talent. Through identification and definition of critical IT and cybersecurity role categories, competency requirements, and career paths, HHS is growing a mature and holistic human capital lifecycle approach.

HHS does not develop role-specific cybersecurity courses, training, or education on a large-scale. It is, however, working to create role-based competency models, career paths, and competency-driven curricula. This curriculum relies on extant training and certification resources, providers, and vendors. This is more cost-effective and sustainable than developing our own, in-house cybersecurity training programs.

Many Federal agencies such as HHS develop ad hoc cybersecurity education, training, and/or curricula even though education and training are not specific to our missions. We do this because our missions would not be possible without our vast and secure applications, systems, and networks. Perhaps those agencies that have specific roles in overseeing and governing the federal workforce should be augmented with specific resources and requisite governance structures to implement a federal-wide cybersecurity workforce education, training, and development program. The Federal government would benefit from a centralized, standardized, streamlined, and cost-effective approach to address this need. This would reduce duplicative and conflicting efforts occurring across Federal Government and foster related government-wide training reciprocities and/or acquisitions. It would also limit the burden on agencies whose primary missions do not include cybersecurity education, training, and curriculum development. Lastly, it will cost less to our taxpayers.

CURRICULUM-BASED EFFORTS AT HHS

Career Paths

HHS is developing career paths for its IT and cybersecurity workforce. These career paths have HHS-specific role definitions and requirements, and are mapped to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF)[1] Specialty Areas and Work Roles. The career paths provide extensive information including:

- Role descriptions and key tasks;
- Preferred degree types and certifications;
- Career mobility paths;
- Competency-profiles, including behavioral indicators across four degrees of proficiency for each competency contained within; and,
- Competency-based learning and development experiences, such as mentoring, rotations, and job shadowing.

These career paths will help HHS strengthen its IT and cybersecurity workforce capabilities. They support curricula and career development for HHS's current and future staff, and provide a basis for role-based, competency-aligned performance management. As HHS continues this effort, the standardized career paths will expedite the recruitment process with standardized PDs and support role-based strategies for professional development and retention strategies.

Certification Alignment

Through its efforts to comply with the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA), the HHS IT and Cybersecurity Workforce Development team conducted a survey across HHS' IT and cybersecurity communities to validate a list of integral, role-based certifications. HHS is currently working across government and with training vendors to crosswalk this certification alignment with the updated NCWF Work Roles. HHS is also developing a Certification Review Board (CRB) process to continually and consistently review certification alignment to HHS IT and cybersecurity work. This

[1] The NCWF is published in the National Institute of Standards and Technology (NIST) Special Publication 800-181.

CRB will comprise subject matter experts (SMEs) from across HHS and its Operating Divisions (OpDivs).

No-Cost Training Catalog

Using available resources, HHS developed a catalog of free IT and cybersecurity training, which is organized by: (1) the top seven certifications identified by the HHS FCWAA 2016 respondents; and, (2) recommended HHS role-specific IT and cybersecurity certifications. These no-cost trainings include options from the Federal Virtual Training Environment and HHS' Learning Management System, to name a few.

GROWING AND SUSTAINING THE NATION'S CYBERSECURITY WORKFORCE

1 QUESTION 1

What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

1.1 METRICS AND DATA FOR CYBERSECURITY EDUCATION, TRAINING, AND WORKFORCE DEVELOPMENT

There are some very effective metrics for measuring the efficacy of education, training, and workforce development, including time-tested models of evaluation like the four levels of the Kirkpatrick Model. These types of metrics have not yet been implemented to the extent that enables us to measure "real" effectiveness in cybersecurity. For example, high schools, colleges or certification training providers collect information about the field of study; theoretical training in cybersecurity; graduation rates; and, pass/fail statistics. They do not, however, provide true insight into the preparedness of individuals to enter or remain in the cybersecurity workforce. We are still unable to effectively link cybersecurity training, education, and workforce development to behavior (level 3) and results (level 4). At level 3 and 4, the following questions would be answered:

- Are the number of incidents reducing?
- Are our response and recovery times improving?
- Do the right career paths, hiring flexibilities, and retention capabilities exist to meet cybersecurity missions?
- Are cybersecurity professionals staying in the field longer, or are they leaving? And, if there is a high level of attrition, to what can that be attributed?

In the Federal space, metrics and measures of efficacy would be beneficial, but the first priority is identifying the authority that will develop these metrics and collect, analyze, and report the data across Federal Government. The lack of strategy in these areas perpetuates inefficiencies in government operations, creates knowledge and learning gaps across agencies, and creates silos of unshared, under-shared, and misappropriated resources. Cybersecurity workforce development, training, and education policy should be standardized across the Federal Government and managed by those agencies that have specific roles in overseeing and governing the Federal workforce. Furthermore, those Departments should promote and enforce that policy across the government, overseeing and supporting its implementation, gathering metrics, and managing related resources.

1.2 IMPROVEMENTS FOR COLLECTING, ORGANIZING, AND SHARING INFORMATION

The Federal Government should consider professionalizing the cybersecurity workforce through standardized career paths, competency models, position descriptions, personnel coding, performance management, and ongoing professional development. This will enable the Federal Government to serve the American public with less duplication of efforts, more consistency across the branches and services, and improved processes.

1.2.1 Define: Career Paths and Competency Models

Career paths and competency models are fundamental to the human capital lifecycle. They also provide the data and metric-driven approach to workforce development that is needed. They help with competency gap assessments, they facilitate targeted staff planning and recruitment, and they can support role-specific, competency-based scenario testing and ongoing development and performance management. The Federal Government should maintain and socialize a set of consistently defined IT and cybersecurity career paths and competency models that align with the NCWF Work Roles. This will facilitate collective (rather than disparate) efforts to comply with current legislation (e.g., the FCWAA). It will also support our ability to collaborate across the public and private sector and academia.

Established and shared career paths and competency models should ultimately inform all related IT and cybersecurity workforce development objectives including workforce planning, recruitment, education, professionalization, succession, and retention. These career paths should be multi-tracked (e.g., Senior Executive Service (SES) trajectory, Senior Leader/Scientific and Professional trajectory, and career lattice opportunities) and include:

- Role-based, competency-based education, training, and professional development recommendations across the grade-level trajectory;
- NCWF alignment;
- Preferred degree types and certifications for performing each Work Role;
- Standardized, role-specific performance management plans for each Work Role;
- Standardized, role-specific individual development plans for each Work Role.

1.2.2 Hire: Position Descriptions, Recruitment, Interviewing, and Onboarding

We cannot train and develop a workforce we do not have. Once all IT and cybersecurity positions are defined, categorized, and analyzed consistently across all departments and agencies, information sharing becomes much easier, as does the recruitment process. If agencies use the same Work Roles, career paths and competency requirements, then position descriptions and qualifying criteria should become transferrable between agencies (e.g., someone who qualifies as a Cyber Defense Incident Responder at one Agency would also qualify for the same role with another Agency without having to requalify). Consistency and reciprocity will reduce the current lag in recruiting, interviewing, hiring, and onboarding a competent IT and cybersecurity workforce.

Shared resources will also reduce redundancy across the Federal Government as all agencies endeavor to implement FCWAA workforce coding procedures. This will enable agencies to better track encumbered and vacant cyber positions with NCWF's Work Role codes and facilitate effective IT and cybersecurity workforce forecasting and planning. This will additionally improve the ability to track development opportunities for each member of the federal IT and cybersecurity workforce. Sharing and adopting standard position descriptions across the Federal Government would additionally reduce the burden on human resource (HR) offices. There is a current backlog in hiring in the Federal Government, crippling its ability to hire the best talent for IT and cybersecurity positions.

The Federal Government's salaries, specifically in regard to IT and cybersecurity roles, are not competitive with private industry. The Federal Government's appeal is its excellence in mission and state-of-the art technology; purpose-driven work is very enticing to the future workforce, which is more driven by the meaning behind the work. HHS is looking for dedicated civil servants from a younger generation, which is very "now-centric" and accustomed to immediacy in technology. It will be much more difficult to recruit this generation with mission and vision, while asking them to endure an extensively long hiring and onboarding process. Unless the Federal Government identifies solutions to share information, hiring practices, resources—even interview practices and hiring standards—we continue to put ourselves at risk for a less-than-adequate workforce to defend the security of America's infrastructure and resources.

1.2.3 Develop: Training, Education, & Professionalization

The Federal Government would benefit from a centralized training, development, and professionalization resources. HHS has been reviewing the Defense Acquisition University (DAU) website (https://www.dau.mil/), for example, and believes our career paths, competency models, and training catalog could be applied to something similar to DAU's established training resource model. Career proficiency levels could be used to delineate each role and create a full career development curriculum for each of IT and cybersecurity Work Role. Such a role-based competency-based training and development repository should be centrally managed, and with proper analysis, design, development, and implementation.

1.2.4 Sustain: Talent Management and Performance Metrics

Agencies can best share resources and information if everyone is working from the same standards. Metrics for success also become easier. If the Federal Government shared and integrated NCWF-aligned competency models and career paths, competency assessment and workforce analytics improves; hiring is streamlined; and, performance management, individual development, and professionalization are role-specific and competency-driven-all of which can be more easily measured.

.

2 QUESTION 2

Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/ skills/abilities?

While the NCWF Categories, Specialty Areas, Work Roles, knowledge, skills, and abilities (KSAs) are a step in the right direction to understanding and categorizing cybersecurity work, there is still confusion regarding:

- the purpose and scope of the NCWF;
- the application of the NCWF; and,
- the utility of the NCWF to track cyber workload and competencies.

2.1 THE PURPOSE AND SCOPE OF THE NICE FRAMEWORK

The definition of a framework is a structure for supporting the whole. By the very definition, a "Cybersecurity Workforce Framework" should not be prescriptive, but rather support cybersecurity workforce efforts. While we require the same skillsets, agencies still require certain flexibilities to accommodate the "true" cybersecurity work and workload balancing that exist within their organizations. Per requirements from the FCWAA, OPM established procedures to implement the NICE coding structure to identify all federal civilian positions that require the performance of IT, cybersecurity, and other cyber-related functions. Implementing this as a prescriptive, one-size-fits-all framework, as required by the law, has led to confusion in using it as a means to identify and address workforce needs (e.g., workload balancing, replacement hiring, contractor-to-federal full-time equivalent (FTE) ratios, etc.).

There is further confusion regarding the scope of the FCWAA and its prescribed use of the NCWF for identifying and defining work beyond cybersecurity. The FCWAA requires agencies to report on IT, cybersecurity, and cyber-related workforce by using the NCWF, but does not define "cyber-related" workforce. Additionally, the titles for FCWAA and NCWF only contain the word "cybersecurity" and do not fully describe the reach to IT and cyber-related. The NCWF's Categories, Specialty Areas, and Work Roles include positions that are not typically found within the IT 2210 Information Security (InfoSec) parenthetical (e.g., network services), and yet the FCWAA requires identification and coding of those positions.

2.2 THE APPLICATION OF THE NICE FRAMEWORK TO THE FEDERAL WORKFORCE

The federal cybersecurity workforce is distributed across multiple occupational series. While, the majority of cybersecurity professionals are hired into the 2210 IT Management Series, there are many that are not. As there is no specific cybersecurity occupational series, this makes it very difficult to track the federal workforce that performs cybersecurity functions in alignment to the NCWF.

Furthermore, the connections between the current cyber-related occupational series, the 2210 parentheticals, and the NCWF are not so clear-cut. Although attempts have been made to clarify this linkage through the use of the Department of Homeland Security's (DHS') PushButtonPD Tool, this tool's usage has not been consistently socialized or applied across agencies. More efforts are needed to increase understanding and communication of aligning the NCWF to relevant IT and cybersecurity occupational series, potentially through the creation of a new and updated occupational series.

Also, we need to focus on building a multifaceted and multidisciplinary workforce that can support all areas of the NIST Cybersecurity Framework (CSF) in both steady-state and emergency-state operations, not just those that respond to incidents as they occur. As such, there needs to be better alignment between the NIST CSF and NIST NCWF.

Additionally, there are 50 cybersecurity/cyber-related roles/titles described across multiple NIST Special Publications, of which, not all can be intuitively mapped to the current iteration of the NCWF. As these roles may not have clear linkages to the NCWF, and as federal departments and agencies are required to align their workforce to the NCWF, there may be a risk that critical roles are overlooked in the government's FCWAA coding efforts. This effort is beyond the scope of HHS' authorities and bandwidth, and will require NIST-coordinated efforts to ensure that all roles described in NIST Special Publications and Frameworks are clearly aligned to the NICE Framework.

Finally, the NCWF was released as draft in November 2016. This version is subject to change after public comment which was due January 2017 and the updated version is scheduled for release by August 2018.

2.3 THE UTILITY OF THE NICE FRAMEWORK TO TRACK CYBER WORKLOAD AND COMPETENCIES

HHS has developed role-based competency models and career paths for its IT and cybersecurity professionals. Historically, HHS has treated the NCWF Specialty Areas as competencies (the aggregate of tasks, KSAs, and behaviors required for successful job performance). Once completed, these competency models will facilitate HHS's ability to conduct more informed and data-driven workload balancing and workforce analytics against the OPM dataset. By treating the Specialty Areas as competencies and by creating competency models, HHS is building the foundations to truly informed workforce analyses.

Currently, OPM has provided guidance that allows organizations to code up to three Work Roles; however, the guidance does not effectively and accurately assist with capturing, accounting, and planning for things such as:

- Workload balancing (e.g., many IT and cybersecurity employees perform across multiple Work Roles and not at the same level of criticality and capacity);
- Replacement hiring; and,
- Contractor FTE and workload balancing (e.g., in a firm-fixed price contract, insights into the number of contractors it took to produce a given deliverable or the mix of those skillsets is skewed at best).

Additionally, as the threshold for grade-determination and classification is 25% of work completed, it was unclear to HHS as to why OPM did not allow agencies to assign up to four different codes to each of their IT and cybersecurity positions.

Lastly, there is not a clear linkage between the cybersecurity work performed across the government and the NCWF Work Roles. HHS conducted several focus groups to determine how its IT and cybersecurity workforce aligns to the NCWF. This effort found additional cybersecurity work in HHS that that is not well-represented in the NCWF (e.g., enterprise risk management, continuous diagnostics and ongoing authorization, and penetration testing).

3 QUESTION 3

Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

3.1 HHS' CYBERSECURITY POLICIES ON WORKFORCE, EDUCATION, AND TRAINING

HHS has some cybersecurity policies in place regarding workforce, education, and training and they are regularly and consistently enforced with authority from law and federal regulation. Both the Federal Information Security Modernization Act (FISMA) and the OPM Regulation 5 Code of Federal Regulations (CFR) 930.301 mandates that federal agencies: (1) identify personnel with significant security responsibilities (SSR); and, (2) provide role-based training (RBT) commensurate with role-based responsibilities.

The HHS OCIO Policy for Information Systems Security and Privacy (IS2P) established Department-wide requirements for protecting the security and privacy of HHS data. The IS2P requires that HHS employees and contractors with SSR receive role-based training commensurate with their roles and responsibilities.

Also under the authority of IS2P, HHS instituted its *Rules of Behavior (RoB),* which include the policy and the rules that govern the appropriate use and protection of all HHS information resources and help to ensure the security of IT equipment, systems, and data and their confidentiality, integrity, and availability. The RoB applies to all Department personnel, contractors, and other information system users. All HHS employees, contractors, and other personnel with access to HHS information and information systems must complete *HHS Information Systems Security Awareness Training* prior to accessing any HHS system and take the training annually thereafter. HHS, under the authority of IS2P, may issue disciplinary action and suspend or revoke access to federal information, information systems, and/or facilities for noncompliance.

In January 2017, HHS responded to the FCWAA of 2015, Pub. Law No. 114-113, 129 Stat. 2936 (2015). This response included:

- Per Sec. 303(b)(1)(D)(i), the percentage of HHS personnel with IT, cybersecurity, and cyber-related job functions who currently hold the appropriate industry-recognized certifications as identified under the NICE;
- Per Sec. 303(b)(1)(D)(ii), the level of preparedness of HHS cyber personnel without existing credentials to take certification exams; and,
- Per Sec. 303(b) (1)(D)(iii), a strategy for mitigating any certifications gaps identified in clause (i) or (ii) with appropriate training and certification for existing HHS personnel.

The following constraints influenced the data collection and our current approach to related cybersecurity training strategies and policies:

- The law requires reporting on "The percentage of personnel with IT, cybersecurity, and cyber-related job functions who currently hold the appropriate industry-recognized certifications as identified under NICE." While the NICE National Initiative for Cybersecurity Careers and Studies online portal provides an education and training catalog, which includes some certifications, no federal standard for industry recognized-certifications exists under NICE. HHS and many other agencies therefore worked separately to generate their own certification lists for this effort. This led to duplication and cost inefficiencies across government.

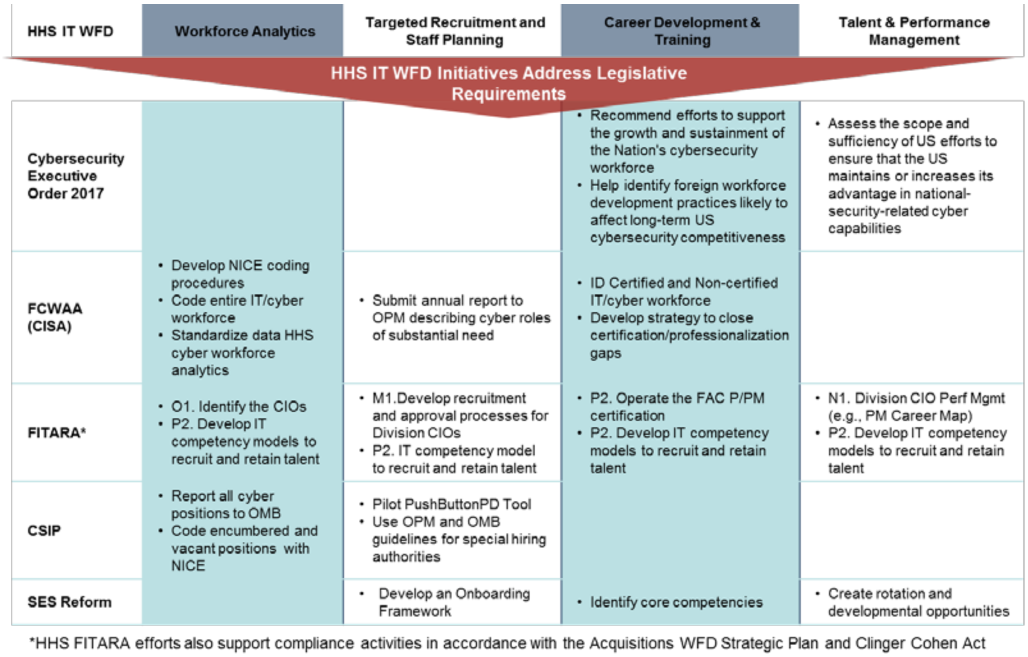
- The FCWAA requires agencies to report on IT, cybersecurity, and cyber-related workforce, but does not define "cyber-related" workforce. Additionally, the title of the law is not fully descriptive of its scope because it includes only "cybersecurity," but the legislative text requires reporting on IT, cybersecurity, and cyber-related workforce. Each agency came up with its own definitions.
- The law only requires reporting on the percent of personnel holding industry-recognized certifications, but does not recognize formal education as a measure of knowledge and capability. A diploma, in essence, is a certificate awarded by an educational establishment to show that an individual has successfully completed a course of study.
- No federal standard was provided for determining the level of preparedness of professionals who currently do not hold industry-recognized certifications. Each agency came up with its own definitions.
- Civilian agencies are not currently authorized to make certifications a condition of employment for this workforce, which spans several OPM occupational series (e.g., IT 2210); thus leaving many departments and agencies without authority to enforce mitigation strategies for closing certification gaps.
- The HHS budget has been allocated through Fiscal Year (FY) 2018, which precludes HHS from dedicating additional training funds to mitigate certification gaps until FY 2019; again leaving many departments and agencies without authority to enforce mitigation strategies for closing certification gaps.

In June 2017, HHS released a memo to update the RBT and SSR requirements stated in the HHS IS2P from every three years to every one year, and align with the NCWF. NCWF Work Roles will help us continue our efforts to comply with the FCWAA while delineating SSR roles and identifying commensurate training and certifications. The goal of the June 2017 RBT memo was to ensure personnel with SSR receive specific skills training and education to develop and maintain a cybersecurity workforce capable of actively reducing and managing risk to HHS information and systems. As noted previously, through its FCWAA efforts, HHS surveyed its Chief Information Officer (CIO) and Chief Information Security Officer (CISO) communities to validate a list of integral certifications for HHS' categories of IT and cybersecurity work. Using available resources, HHS compiled a list of free training courses that aligned to those certifications, and therefore the role categories. This catalog of role-based training options was delivered with the updated HHS RBT memo in June.

Under the FCWAA, departments and agencies are also required to identify and code all encumbered and vacant positions with IT, cybersecurity, and other cyber-related functions (as defined by the NCWF structure). On January 4, 2017, OPM released a Guidance Memo, in accordance with the FCWAA, that directs agencies to establish procedures for identifying and coding their encumbered and vacant IT, cybersecurity, and cyber-related positions and to implement those coding procedures with the updated NCWF Work Role codes by April 2018. HHS OCIO and the OHR collaborated to develop HHS-specific guidance which provides the Department, including Staff Divisions (StaffDivs) and OpDivs, with specific instruction for coding positions. Per this HHS-specific guidance, each StaffDiv and OpDiv is charged with further defining specific coding guidance and instructions for their organizations and is directed to begin internally reporting on their coding efforts in FY 2018. The FCWAA mandates coding of IT, cybersecurity, and cyber-related positions and gives HHS' OHR the authority to enforce Department-specific guidance.

3.2 HHS' DEPARTMENT-WIDE CYBERSECURITY WORKFORCE DEVELOPMENT GOVERNANCE

HHS institutionalized an IT and Cybersecurity Workforce Development Working Group (WFD WG) in 2015 to address the workforce legislative demands and requirements like the FCWAA. As depicted in Figure 1, these legislative requirements extend across the human capital lifecycle—workforce analytics, targeted recruitment and staff planning, career development and training, and talent and performance management.



HHS IT WFD Initiatives Address Legislative Requirements

HHS IT WFD	Workforce Analytics	Targeted Recruitment and Staff Planning	Career Development & Training	Talent & Performance Management
Cybersecurity Executive Order 2017			• Recommend efforts to support the growth and sustainment of the Nation's cybersecurity workforce • Help identify foreign workforce development practices likely to affect long-term US cybersecurity competitiveness	• Assess the scope and sufficiency of US efforts to ensure that the US maintains or increases its advantage in national-security-related cyber capabilities
FCWAA (CISA)	• Develop NICE coding procedures • Code entire IT/cyber workforce • Standardize data HHS cyber workforce analytics	• Submit annual report to OPM describing cyber roles of substantial need	• ID Certified and Non-certified IT/cyber workforce • Develop strategy to close certification/professionalization gaps	
FITARA*	• O1. Identify the CIOs • P2. Develop IT competency models to recruit and retain talent	• M1.Develop recruitment and approval processes for Division CIOs • P2. IT competency model to recruit and retain talent	• P2. Operate the FAC P/PM certification • P2. Develop IT competency models to recruit and retain talent	• N1. Division CIO Perf Mgmt (e.g., PM Career Map) • P2. Develop IT competency models to recruit and retain talent
CSIP	• Report all cyber positions to OMB • Code encumbered and vacant positions with NICE	• Pilot PushButtonPD Tool • Use OPM and OMB guidelines for special hiring authorities		
SES Reform		• Develop an Onboarding Framework	• Identify core competencies	• Create rotation and developmental opportunities

*HHS FITARA efforts also support compliance activities in accordance with the Acquisitions WFD Strategic Plan and Clinger Cohen Act

Figure 1: IT and Cybersecurity Legislation

HHS's WFD WG and overall WFD program are also grounded in the human capital lifecycle, which facilitates integration of all IT and cybersecurity workforce-related requirements under one strategic effort to reduce duplicative efforts and ensure workforce strategies are fully aligned across HHS. The WFD WG is led by a collaborative partnership of Department leaders, and strategic objectives are executed by SMEs across human capital, IT, and cybersecurity. More specifically:

- **Executive Sponsorship:** Provides oversight and sanctions the WFD WG to executive goals, objectives, and tasking defined in the Strategic IT and Cybersecurity Workforce Development Implementation Plan.
- **Strategic Oversight and Planning:** Oversees overall IT Workforce Planning and Development program strategy and implementation activities; manages implications within the respective OCIO and OHR organizations to include strategy, personnel, infrastructure, requirements, policy enforcement, and other resources. Maintains governance frameworks and supporting management structures to ensure consistency with applicable laws and regulations and adherence to HHS policies, internal controls, and business objectives.

- **Co-Sponsor**: Oversees day-to-day implementation activities and provides technical expertise and integration support to the Coordinator(s).
- **Coordinator**: Plans, organizes, and executes the overall short-, mid-, and long-term implementation activities, directly overseeing completion of tasks in accordance with a defined schedule.
- **Implementation Team Member**: Collaborates with the Coordinator to complete the implementation activities. Members are representatives from across the Department.

4 QUESTION 4

What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

4.1 VALUED KNOWLEDGE AND SKILLS

HHS-valued IT and cybersecurity KSAs are provided in Appendix A. The Department identified 29 IT and cybersecurity role categories and their related competency requirements for successful job performance.

HHS elected to use the NCWF's Specialty Areas as technical competencies. HHS chose this approach because each NCWF specialty area includes a set of tasks and KSAs, and by definition, a competency is a set of related KSAs and behaviors required for successful job performance. HHS then developed corresponding behavioral indicators (BIs) to compile a comprehensive profile for each technical competency.

The HHS IT and Cybersecurity Workforce Development team identified its IT and Cybersecurity role categories in coordination with Department IT and cybersecurity SMEs and leadership (Appendix A). HHS agrees these are the general types of work and competency requirements for successful IT and cybersecurity job performance. These role categories have recently been updated to align with the NCWF Work Roles. HHS' role category definitions, NCWF alignment, and competency alignments have been shared with the broader federal IT, cybersecurity, and human capital communities, who acknowledge the comprehensive scope of the work represented. HHS' framework for competency models and career paths align to the Federal Information Technology Acquisition Reform Act (FITARA) and the FCWAA (i.e., NCWF). This model is now being adopted and tailored by OPM for federal-wide use.

4.2 REALISTIC EXPECTATIONS

HHS' IT and cybersecurity role categories, definitions, and associated competency requirements were modeled after the "actual" IT and cybersecurity work performed across the Department. These definitions and competency requirements are: (1) based on NCWF specialty area KSAs; and, (2) provide a standardized platform to plan for current and future staff needs, assist in targeted recruitment efforts, and support multi-track role-based career development.

As HHS identified the competencies for successful job performance, it also developed BIs for manifesting each competency. These BIs were calibrated across four degrees of proficiency, and proficiency targets were set based on career levels. Through these efforts, HHS has set realistic expectations for its workforce. Though HHS' expectations are realistic, workforce shortages frequently require people to perform multiple functions across multiple levels to ensure that work is performed well. HHS' IT and cybersecurity workforce is highly skilled, but unfortunately, understaffed.

From our experience in recruitment efforts with CyberCorps: Scholarship for Service and collaboration with Centers of Academic Excellence (CAE), HHS' expectations for knowledge and skills are aligned with established curriculum. However, hiring officials frequently seek candidates with previous work experience and on-the-job training because the current shortage in the IT and cybersecurity workforce continues to increase workload demands on existing staff. As a result, hiring managers and their teams do not have the time or capacity to indoctrinate new and inexperienced staff. HHS' current recruitment efforts target applicants with 2-3 years of relevant work experience. This trend also lends to the continual "swapping" or "poaching" of IT and cybersecurity staff among Department and Agencies.

4.3 ROLE, INDUSTRY, AND SECTOR VARIANCES

IT is a critical enabler to patient-centric healthcare and human services. Multiple business demands, coupled with vast and evolving legislative requirements, drive our healthcare-related IT and cybersecurity initiatives and workforce needs. This challenge, however, is not specific to this industry. The world runs on ever-evolving and innovative IT, and IT is run by people. This infrastructure must be protected by a multi-faceted, multi-disciplinary workforce with the agility, collaborative spirit, and disposition to stay ahead of the technological advancements and evolving threats within any environment they're charged to protect (e.g., healthcare, automotive, defense, etc.).

The federal shortage for critical IT and cybersecurity capabilities exists across all industries and sectors. The talent pipeline simply is not there. This systemic, macro-level gap must first be addressed before we start targeting more nuclear, industry-based skillsets required across this workforce. The Federal Government must focus its attention on increasing the general IT and cybersecurity workforce before developing niche areas, as all areas of industry require a capable IT and cybersecurity workforce to do business securely and efficiently.

5 QUESTION 5

Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

5.1 MOST EFFECTIVE PROGRAMS

The most effective cybersecurity education, training, and workforce development programs empower the workforce to excel in their role. They are governed effectively, have updated policies, provide ample training and development opportunities, and promote higher education. Effectiveness should be monitored through metrics on attrition, knowledge attainment, role-based scenario-based competency testing, an organization’s ability to meet the objectives of the CSF, and employee viewpoint surveys.

The strongest cybersecurity workforce development programs take a holistic approach to the entire CSF, and recognize that the goal of cybersecurity is to prevent the incidents from happening in the first place. It is equally important to focus on the front-line skillsets of policy developers, system and network administrators, and risk managers, as it is to focus on the special operations digital media analysts, and incident response teams.

Workforce development initiatives must focus on more than skills development of high-visibility staff such as penetration testers and cyber analysts. They must give credence to a team-based approach, while focusing on the entire human capital lifecycle (e.g., analytics, recruitment, development, talent and performance management) for the entire IT and cybersecurity workforce. The ultimate result is skilled cybersecurity and IT teams with a disposition and aptitude for critical thinking, problem solving, communications, and teamwork.

The most effective learning and development programs use a whole-person approach for training, education, and performance management with the understanding that developing cybersecurity skills, along with leadership, communication, and administration skills most benefit the worker and the organization. They implement and maintain effective, time-tested professional development initiatives including apprenticeships, mentorships, job shadowing, and job rotations. They work to build the workforce holistically, focusing not only on technical skills, but soft skills that develop teams, relationships, and communications.

Gamification is another time-tested training, development, and recruitment tool proven to be very effective with the IT and cybersecurity workforce. Capture the flag games, simulations, cyber wars, and other cyber challenges are excellent ways to train employees, develop skills, and provide a simulated real-time emergency for threat response.

5.2 GOALS FOR PROGRAMS & MEASURES OF SUCCESS

When determining programs and measures of success, the best cybersecurity workforce development programs will focus on the Three Pillars (The Three E’s):

- **Ethics (White Hats)**: Effective ethics practices will focus on providing incentives to keep the staff “white hat.” Ethical practices will provide meaningful and motivating rewards to staff above and beyond salary and benefits; they will emphasize top prevention strategies and promote white hat behaviors.
- **Environment (Centers of Excellence)**: Environment fosters the cybersecurity workforce’s ability to win as cyber defenders. In the right environment, there is a seamless integration of strategy and execution, where objectives and performance measures are aligned organizationally. There is a commitment to providing streamlined, on-demand access to resources needed for innovation and rapidly adaptive cyber-defense. And finally, a healthy environment focuses on building leaders, not “managers,” and not low-performers. In other words, the rewards for leadership and development are high, which encourages the best performers and leaders to continue in high performance.

- **Economics (Efficiency of Labor Supply = Labor Demand)**: Highly-skilled talent is urgently needed—tech advances are accelerating the need for human-led advanced threat defense, analysis, and mitigation. The Federal Government should consider a hiring schedule (Non-GS) that accounts for this unique market and extremely limited pool of qualified talent. Additionally, for this particular workforce, a staffing model blending in-house and outside services may offer solutions. The Federal Government could also study international talent pool engagement options.

5.3 EXAMPLES OF EFFECTIVE PROGRAMS

HHH' IT and cybersecurity workforce development program meets current and future business needs through the requisite education, training, and increased technical expertise to respond to emerging threats and evolving cybersecurity requirements. HHS launched a comprehensive IT Cybersecurity Workforce Development Program, which focuses on five major areas for identifying, defining, acquiring, developing, and sustaining a strong IT cybersecurity workforce: 1) strategic planning and governance; 2) role-based workforce analytics and planning; 3) targeted recruitment and staffing; 4) career development and training; and, 5) talent and performance management.

The HHS IT cybersecurity career path model is foundational to these efforts. This model includes role-specific definitions, technical competency models, career mobility models, and competency-based learning and development. It is designed to be sustainable, repeatable, and customizable; and it aligns directly to the NCWF. HHS' established a methodology accommodates and supports its growing IT and cybersecurity workforce, while adapting to federal initiatives and requirements.

HHS' IT Strategic Plan prioritizes workforce development as the number one priority among its mission-critical efforts. Building and retaining talent requires increased efforts specifically targeting both educating and engaging the workforce.

HHS is piloting a new IT/Cyber-focused job rotation initiative and is building a mentoring program. The rotation and mentoring program, together, comprise HHS' new "Partners in Excellence" program. This new initiative will help develop technical talent in our workforce and empower them to move their careers and their skills in the direction they choose.

6 QUESTION 6

What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

6.1 CYBERSECURITY EDUCATION, TRAINING, AND WORKFORCE DEVELOPMENT CHALLENGES

We found that workforce shortages and continually-increasing workloads often create an imbalance that hinders employees' ability to attend training or obtain certifications. While federal departments and agencies are working to identify new methods for recruiting critical IT and cybersecurity positions through direct hire, internships, Schedule A, and targeted recruiting through CAE universities and professional organizations, this still isn't enough. The majority of federal IT and cybersecurity staff is at the GS-13 or higher. From federal workforce data gather through FedScope, CEB Inc. (now Gartner) found that millennials only make up 7% of the federal workforce, and the average age of our current federal IT and cybersecurity workforce is over 40. The pipeline of IT and cybersecurity talent remains inadequate, and federal agencies struggle to compete in the hyper-competitive market for talent. Complicated, federal-wide government HR processes and legislation hinder federal recruitment, hiring, and retention efforts, and lack of compensation flexibilities leave us ill-equipped to compete with private industry. The overall IT spend at HHS is one of the largest in the government. Without significant, ongoing investment in and commitment to people, we don't just run the risk of losing a return on our technology investments. We jeopardize the Department's ability to effectively protect the health of all Americans and provide essential human services.

In 2015 millennials surpassed the Gen Xers as the largest generation segment in the U.S. labor force.[2] Federal departments and agencies struggle not only to compete with private industry for qualified candidates, but also to offer equitable compensation packages and onboard new employees in a timely fashion. Title 5 of the CFR, and other hiring flexibilities like Direct Hire Authority, do not provide enough flexibility to adapt to this rapidly-changing labor market and integrated workforce. The CFR and its 50 titles were first published in 1939 and do not address today's need to hire a new generation of workers who prefer the diverse challenges of short-term, project-based work.

Additionally, the Federal Government as a whole, does not have a consistent mechanism to identify and code the IT and cybersecurity workforce. The FCWAA attempts to do this through the NCWF, but it is still in draft and does not address all of the roles represented across the NIST publications. This complicates the ability to properly identify the workforce, understand resource and skill gaps, line-balance staff to mission-critical needs, and properly project and plan for future demands. The absence of data-supported decisions stifles the natural flow of the human capital lifecycle and ultimately hinders the Federal Government's ability to build a fully staffed and capable IT and cybersecurity workforce.

The Government is bound by duplicative and conflicting workforce legislation. At HHS, the IT and Cybersecurity Workforce Development Strategic Plan goals and implementation teams align to the regulatory requirements, yielding efficiency and consistency in compliance processes. However, the system continues to be bogged down with tracking and reporting requirements and in most cases, using different coding and reporting schemas. For example, under the Cybersecurity Strategic Implementation Plan (CSIP), the Office of Management and Budget (OMB) and OPM required departments and agencies to code IT and cybersecurity positions using the NCWF in 2015. A year later, the FCWAA required similar position coding effort, but changed the NCWF structure, making the CSIP coding results obsolete.

6.2 CYBERSECURITY EDUCATION, TRAINING, AND WORKFORCE DEVELOPMENT OPPORTUNITIES

The NCWF provides a solid foundation for identifying and tracking the IT and cybersecurity workforce. NIST and OPM intentionally provided open and flexible guidance for implementing the NCWF codes, aligning encumbered and vacant IT and

[2] http://www.pewresearch.org/fact-tank/2015/05/11/millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force/

cybersecurity positions to Work Roles and allowing departments and agencies to adapt guidance to organizational needs. However, there is an opportunity for NIST and OPM to develop specific guidance and protocol for coding positions, leading to consistent identification of knowledge, skills, and abilities. This in turn will foster a federal-wide view of the IT and cybersecurity workforce and provide a mechanism to define competencies, target recruitment, identify training and education needs, and hone professional development and retention strategies.

Additionally, the NCWF provides a basis to establish additional classification standards to the 2210 Information Management Series that is the most commonly-used series for IT and cybersecurity positions. Currently, the outdated classification and qualification standards handicap the ability to account for the full scope of work or develop evaluation reviews that reflect complex IT and cybersecurity duties. Using the NCWF Work Roles, there is an opportunity to incorporate the defined knowledge, skills, and abilities into the 2210 factor-level descriptors and the overall job family standard. This will support consistent recruiting and hiring across government and provide HR professionals with the authority to develop accurate and comprehensive classification and hiring artifacts for IT and cybersecurity positions. As it stands, the federal HR community is fearful of an audit. Unless they are given true authority to inject the NCWF into the OPM 2210 qualification and classification standards, we'll remain at a confusing impasse between HR and hiring managers.

Lastly, there has been a growing legislative trend in which defense and intelligence departments and agencies are granted special hiring flexibilities or recruitment and retention incentives for their IT and cybersecurity workforce. Those KSAs found at DHS are also found at HHS, yet HHS does not have the same hiring mechanisms to bypass Title 5's antiquated requirements. Given that the same demand exists for IT and cybersecurity professionals across the Federal Government, special hiring authorities and flexibilities should be granted to all departments and agencies (e.g., the DHS Cybersecurity Workforce Assessment Act 113-246 or the Border Patrol Agent Pay Reform Act 113-277).

7 QUESTION 7

How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

7.1 ADVANCES IN TECHNOLOGY

The inevitability of technological advancement and the unpredictability of the types of advancement or the impacts thereof, make it difficult to predict how those changes will impact the workforce of the future. The coming workforce is so different than previous generations that it, too, is a challenge to predict and plan.

Change is coming, which will require not only a change in technology, but in processes, required competencies, policies, the way we recruit and hire, and the types of security we implement. And, while all those things will change, the required skills of analysis, strategic thinking, problem-solving, technical and mental acuity, and adaptability remain the same.

A heart surgeon certified 50 years ago, is a heart surgeon today, changes in technology and techniques notwithstanding. An information security officer of 10 years ago is an information security officer of today, changes in technology and techniques notwithstanding. The competencies that surgeon developed through their education and practice remain the same. While the technology changes and the methods for procedures have been modified, with professional continuing education, that heart surgeon can continue to save lives.

Cybersecurity is cybersecurity. It was cybersecurity 10 years ago, and it will be cybersecurity in 10 years. Technology, adversaries, approaches, and outcomes change, but each Work Role's (e.g., cybersecurity policy analyst, intelligence analyst, computer network defender) core competencies will not change. The tools they use will change. That is why we recommend that we consider professionalizing the IT and cybersecurity workforce, analogous to healthcare providers, lawyers, etc. Therefore, we believe that technological changes are less of a factor than, for example, how we hire and manage our workforce when it comes to the future workforce needs and demands.

Additionally, the way the future workforce interacts with each other, technology, and society is so distinct, that the programs we use to educate, train, and develop them will require an overhaul to keep the federal workforce operating at its best, improving, fortifying, and ensuring the safety and well-being of our nation.

7.2 REFORM ON TITLE 5

Again, we cannot train or develop a workforce that we do not have. The policies contained in Title 5 of the CFR were written before the IT revolution and are archaic in light of best practices now.

"Although the current federal personnel management system is based on important core principles, those principles are operationalized in an inflexible, one-size-fits-all-system of defining work, hiring staff, managing people, assessing and rewarding performance, and advancing personnel. These inherent weaknesses make support of DoD's mission complex, costly and ultimately risky."[3]….

While this quote was about the DoD, it is applicable to every agency in the Federal Government. Reform on Title 5 will be imperative to change, adapt, and remain competitive. "This includes how we attract, develop and support the department's most valuable asset--its people."[4] Reform on Title 5 must focus on how we work with technology through innovation, making space for career flexibility, processes, efficiency, and diversity.

The workforce of the future will work differently and require updated practices, legislation, and work environment. As such, Title 5 must be updated and reformed to take into account the current and future workforce.

[3] http://www.defenseone.com/business/2015/09/pentagon-civilian-worker-reclassification-draws-fire/121094/

[4] http://www.defenseone.com/business/2015/09/pentagon-civilian-worker-reclassification-draws-fire/121094/

7.3 OTHER FACTORS AFFECTING THE FUTURE WORKFORCE

Additional factors affecting the future workforce include, fundamentally, how we address cybersecurity as separate from security. Cybersecurity is not something we practice just at work. It permeates nearly every area of our lives from entertainment to banking, from correspondence to medical care. Many training and education programs treat cybersecurity as a separate area of practice without recognizing the need to address cyber education and development from a whole-person approach.

Cybersecurity training needs to be implemented in our primary education from kindergarten up. By the time individuals enter the workforce, cybersecurity should be as second nature as, for example, locking your front door when you leave your house. With this type of real-life, whole-person cybersecurity education and training, by the time the next generations enter the workforce, they will have core skills, critical thinking skills, and understanding of the digital world in a way that generations past have not. The way future generations work and interact with others will affect the way we plan, manage, and develop the workforce of the future.

The way we approach and train cybersecurity must adapt for the new era in which we live. The Federal Government, and even private industry, needs to allocate resources toward educating and training their current and future workforce first instead of making training and education budgetary afterthoughts. If we don't make training and education priorities in workforce development, we'll suffer not only a shortage in available staff resources, but we are likely to have an under-trained workforce unable to appropriately prevent or to adversaries and risk. Required core competencies will not change in how they are defined. Technology and environmental changes, however, make it vital for organizations to provide constant, effective training and education programs for all of their staff.

Additionally, the way we hire and govern our workforce will need to change as Generations X and Y occupy the senior management and leadership roles. Baby boomers today are 54-70 and make up 29% of the current workforce. They are going to be retiring in the next 5-10 years. The next generations will require different care and feeding.

- **Workforce Structure**: 65% of millennials said they felt rigid hierarchies and outdated management styles failed to get the most out of younger recruits.[5]
- **Top attractors for graduates and young professionals**: learning development, innovation, and purpose
- **Focus on the future**: employers must emphasize education, communication, engagement, and internal mobility
- **Telework**: "face to face" may be virtual

There is an approaching workforce gap reaching into the millions. One of the best ways we can overcome that gap is to work harder to reach underserved individuals, looking for those with technical aptitudes for strategy, technology, analytics, and mental acuity/behavioral analytics.

[5] https://www.pwc.com/gx/en/managing-tomorrows-people/future-of-work/assets/reshaping-the-workplace.pdf

And, perhaps most importantly, even as technology advances, so will the need for individuals to govern and manage the technology and staff. We will need skilled personnel to govern, write policy about how technology is procured and integrated with other systems, implement, and manage programs and policies over time. We'll need strong acquisitions staff, as well. The demand for future workforce goes beyond just technically trained individuals; it includes strategically, analytically-minded people to ensure the operations, governance, and secure oversight of the IT systems and operations.

Finally, as we look to the future, the Federal Government and the profession of cybersecurity must focus on recruiting a more diverse workforce for IT and cybersecurity positions. Implementing apprenticeship programs, focusing on CAEs with high-diversity profiles, and developing the workforce of the future in areas of lower socio-economic status will help diversify the talent. This will ultimately bring about a variety of perspectives, talents, and strengths we desperately need to face the adversaries of the future.

7.4 MODERNIZATION OF CYBER PHYSICAL SYSTEMS

The modernization of Cyber Physical Systems will call for changes in many areas, with an emphasis on ethics. We cannot predict what sorts of changes will be required in workforce development, but we can predict that there will be a demand for increased cybersecurity defense complexity and a workforce that will need to be able to keep up with that demand. An increase in the connectivity of cyber and physical infrastructure, increased distribution of these systems, and rapidly changing technology requirements will require a workforce with new and changing skills.

Professional development programs will need to provide new, evolved, and more sophisticated black- and grey-hat opportunities. While there is sure to be an increase in automation of a number of cybersecurity processes (e.g., scanning, log reviews, etc.), the changing types of security risks (e.g., botnets, mass cyber-attacks, infrastructure threats) will require cyber defense and offense that is strategically and tactically ready to secure our infrastructure and protect our resources.

8 QUESTION 8

What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

8.1 FEDERAL LEVEL EFFORTS

As its mission is to serve the American people, the Federal Government must be on the forefront to ensure that there is a dedicated workforce capable of protecting American interests in cyberspace. This is essential, as cyber is woven into every aspect of our lives, especially as it relates to healthcare. The Federal Government should lead efforts for growing and sustaining the workforce in the public and private sectors, as well as coordinate efforts with academic institutions to ensure that training and education standards are preparing the next generation with the necessary knowledge, skills, and abilities to perform this daunting task. The Federal Government should lead this effort by:

- Standardizing and centralizing all related efforts through strengthened governance and oversight;
- Improving the NCWF;
- Increasing reciprocity between departments and agencies; and,
- Working with technology providers and academia to prepare for the future.

8.1.1 Strengthening Governance and Oversight

Workforce education, training, and development oversight for the federal IT and cybersecurity workforce is derived from multiple laws, regulations, and initiatives.[6]

Legislative requirements span across the human capital lifecycle—workforce analytics, targeted recruitment and staff planning, talent and performance management, and career development and training—but individually address small segments of the IT, cybersecurity, and cyber-related workforce. For example, FITARA narrows competency development to just the IT program and project managers, and the SES Reform Act focuses on leadership development and accountability.

Governance and oversight for IT and cybersecurity workforce development, inclusive recruitment, education, training, and professional development should be centralized to one organization (or select few) with the authority to enforce, staff, and fund requirements and drive consistency across the entire IT, cybersecurity, and cyber-related workforce. Unifying governance and oversight provides an opportunity to address redundancies and inefficiencies across government while saving our taxpayers' money.

8.1.2 Improving the NCWF

Future iterations of the NCWF should provide greater details about the scope and clarification of the more ambiguous types of cyber work that must be coded according to the FCWAA. Furthermore, the NCWF should provide clearer linkages between positions and roles mandated in other NIST Special Publications and the NCWF. One potential method for improving this would be the creation of a cybersecurity occupational series that takes into account all NIST-required positions and the NCWF.

Federal-level governance, including workforce planning policies and directives, IT infrastructures, and consistently-defined roles and responsibilities for cybersecurity workforce planning have not been established to assist with utilizing the NCWF for coding. An overarching, federal-level data collection and analysis plan is desperately needed. For example, standardizing a list of position titles aligned to and consistent with NIST and OPM guidance for the NCWF would assist with having consistent and reliable definitions of the type of work being performed.

Otherwise, data-collection is not likely to be of consistent quality across all departments and agencies when it is rolled up and reported, and it will not likely support the analysis and planning for which OPM wants to use the data.

[6] Clinger-Cohen Act, E-Government Act , Acquisition Workforce Development Plan , OMB 25-Point Plan for IT Reform, OPM-Issued Guidance for Developing IT Program Managers, OMB CSIP, FITARA, Cybersecurity Information Sharing Act, FCWAA, Cybersecurity National Action Plan, SES Reform Act.

Additionally, departments and agencies need federal-level people, processes, standards, tools, and technologies to effectively and accurately comply with these types of data requests. As data calls increase, the brunt of this work currently rests heavily on cybersecurity hiring managers, and they are currently focused on other national-level data calls and critical cybersecurity missions/operations. The irony here is that we must think of the impact to cybersecurity managers who are already understaffed and need to focus on our cybersecurity missions.

8.1.3 Increasing Reciprocity between Departments

Policy about workforce development, education, and training needs to be standardized across the Federal Government and managed by those agencies that have the specific role of overseeing and governing the federal workforce. The lack of strategy in these areas perpetuates inefficiencies in the government operations, creates knowledge and learning gaps across agencies, and creates silos of unshared, under-shared, and mishandled resources.

Career paths across the Federal Government should clearly and consistently define IT and cybersecurity categories of work and align that work with the NCWF. It would benefit efficiencies, collaboration, training, and overall workforce development efforts to have all agencies and departments sharing the same career paths and competency models for cybersecurity and IT positions. There are numerous benefits including:

- Streamlined recruiting, hiring, managing, and developing processes across the federal IT and cybersecurity workforce;
- Consistent position descriptions, personnel coding, performance management goals, and professional development initiatives; and,
- Ability to work from the same list of integral, requisite, and/or preferred credentials and certifications for each Work Role, and have those credentials and certifications mapped to each position.

8.1.4 Working with Technology Providers and Academia to Prepare for the Future

The inevitability of technological advancement and the unpredictability of the types of advancement or the impacts thereof, make it difficult to predict how those changes will impact the workforce of the future. The coming workforce is so different than previous generations that it, too, is a challenge to predict and plan. The predictability of change demands not only a change in technology, but in processes, required competencies, policies, the way we recruit and hire, and the types of security we implement.

The future workforce, regardless of technology advancement or modernized cyber physical systems, will require different ‘care and feeding’ than previous generations, from recruitment to career development opportunities. Research indicates that the top attractors for graduates and young professionals are: 1) learning development; 2) innovation; and, 3) purpose. The Federal Government and even private industry need to allocate resources toward educating and training their current and future workforce first instead of making training and education budgetary afterthoughts.

The policies and programs we use to educate, train, and develop the workforce require an overhaul to keep the federal workforce operating at its best, improving, fortifying, and ensuring the safety and wellbeing of our nation. If we don’t make training and education priorities in workforce development, we'll suffer not only a shortage in available staff resources, but we'll also likely have an under-trained workforce unable to appropriately respond to adversaries and risk.

Real-life, whole person cybersecurity education and training will provide the future workforce with core skills, critical thinking skills, and understanding of the digital world required to thrive in a technology advancing/changing Federal Government. We must pour efforts into recruiting a more diverse workforce for cybersecurity and IT positions.

8.2 STATE/LOCAL LEVEL EFFORTS

While DHS is primarily responsible for coordinating efforts with state and local governments, HHS has worked with local schools in the past to promote IT and cybersecurity education. Over the past eight years HHS has worked with the Federal CIO Council and Junior Achievement to develop a Job Shadow Day where local college and high school students come to HHS, hear lectures about IT and cybersecurity as practiced at HHS, take a tour of HHS's Operations and Media Center, participate in roundtables with cyber experts, and learn tips for improving their resume to move into an IT or cyber career.

8.3 PRIVATE SECTOR EFFORTS

HHS relies on contractor support for some of its responsibilities. While not currently required, many federal departments and agencies foresee that contractor capabilities will soon need to be tracked, as federal employees are currently required to be tracked by the FCWAA. While current law does not allow for requiring specific training and certification for federal staff, contractors can and should be required to possess all required KSAs to be able to perform the job. Standard contracting language should be updated to ensure that all contractors have credentials and certifications meeting similar standards to the DoD Directives 8570, now 8140.

8.4 EDUCATION AND TRAINING PROVIDER EFFORTS

Education and training providers should team up with the Federal Government for mentorship activities. As noted above, HHS partnered with Junior Achievement and was able to bring a group of high school students to HHS Headquarters where they were able to gain great advice and learn about what a day in the life of and IT and cyber professional is like. High schools and colleges should look to establish such partnerships.

An additional method of this could be through alumni networks. Several federal agencies have had ambassador programs where alumni serve as liaisons to a federal agency and work with university career services to help students find federal work.

8.5 TECHNOLOGY PROVIDER EFFORTS

Technology providers should work with the Federal Government to ensure that their specific systems and certifications align to the NCWF.

APPENDIX A – HHS WORK ROLES FOR IT AND CYBERSECURITY

In some cases, tasks from the 2012 Homeland Security Advisory Committee (HSAC) Task Force on CyberSkills were used.

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
1 Applications Software Specialist	Designs, documents, develops, modifies, tests, installs, implements, and supports new or existing applications software. Functions commonly performed include: • Analyzing and refining systems requirements • Translating systems requirements into applications prototypes • Planning and designing systems architecture • Writing, debugging, and maintaining code • Determining and designing applications architecture • Determining output media/formats • Designing user interfaces • Working with customers to test applications • Assuring software and systems quality and functionality • Integrating hardware and software components • Writing and maintaining program documentation • Evaluating new applications software technologies • Ensuring the rigorous application of information security/ information assurance policies, principles, and practices to the delivery of application software services	• Application Penetration Tester (HSAC Task) • Customer Service and Technical Support (NICE Specialty Area) • Information Assurance Compliance (NICE Specialty Area) • Secure Coders and Code Reviewers (HSAC Task) • Security Engineers - Operations (HSAC Task) • Security Engineers/Architects for building security in (HSAC Task) • Software Assurance and Security Engineering (NICE Specialty Area) • System Administration (NICE Specialty Area) • Systems Development (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Systems Security Analysis (NICE Specialty Area) • Systems Security Architecture (NICE Specialty Area) • Technology Research and Development (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
2	Chief Information Officer (CIO)	Provides leadership on high priority projects, engages in strategic IT investment planning, and drives change across the organization. Provides technical leadership, management direction, overall IT planning, and reliability of internal HHS IT infrastructure systems operated by the HHS CIO as shared services for all services, staff Offices, and regions. Ensures the HHS IT infrastructure is consistent with industry best practices and a comprehensive solution for delivery, and consistent and continuous improvement of infrastructure technology services. Sets performance standards, evaluates performance and overall effectiveness in meeting the Department's IT goals and objectives. Administers enterprise-wide IT policies, procedures, and standards - overseeing programs designed to develop and implement policies and procedures governing HHS IT. Works with other strategic leaders throughout government and in the private sector to challenge conventional approaches, develop innovative IT solutions, and serve as a strategic catalyst to HHS senior management for developing infrastructure solutions and enhancements that will support delivering mission programs and services. Manages relevant IT implications, and represents and speaks for HHS in dealing with key HHS officials, other agency officials, representatives of business and industry, Congressional committees and staffs, and others about plans, programs, policies, and objectives of the OCIO; exercising broad discretionary authority in making on-the-spot decisions and commitments.	• Computer Network Defense Analysis (NICE Specialty Area) • Cyber Operations (NICE Specialty Area) • Threat Analysis (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Information Assurance Compliance (NICE Specialty Area) • Information Systems Security Operations (NICE Specialty Area) • Security Program Management (NICE Specialty Area) • Strategic Planning and Policy Development (NICE Specialty Area) • Systems Security Analysis (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Regulatory Requirements (standards, guidelines, and requirements - derivative of NICE Specialty Area: Legal Advice and Advocacy)

HHS IT/Cybersecurity Work Role		Work Role Definition	Technical Competencies (NICE Specialty Areas)
3	Chief Information Security Officer (CISO)	Serves as senior-level executive responsible for establishing and maintaining the enterprise’s vision, strategy, and program to ensure information assets are protected. Provides comprehensive, senior-level management in the areas of information assurance, security, and privacy. Acts as senior most advisor to the CIO on issues related to information security and privacy. On a continuous basis, evaluates overall IT security direction of HHS through collaborative relationships with OpDiv/StaffDivs and HHS Office of Information Security leaders. Administers enterprise-wide IT security and privacy policies, procedures, standards, and risk management and compliance programs - overseeing programs designed to develop and implement policies and procedures governing HHS information security. Directs staff in identifying, developing, implementing, and maintaining security processes across the organization to reduce risks to information and IT and is adequately prepared to respond to incidents. Oversees compliance for organization. Manages relevant security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.	• Computer Network Defense Analysis (NICE Specialty Area) Cyber Operations (NICE Specialty Area) • Threat Analysis (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Information Assurance Compliance (NICE Specialty Area) • Information Systems Security Operations (NICE Specialty Area) • Security Program Management (NICE Specialty Area) • Strategic Planning and Policy Development (NICE Specialty Area) • Systems Security Analysis (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Regulatory Requirements (derivative of NICE Specialty Area: Legal Advice and Advocacy)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
4	COMSEC Manager	Oversees the installation, implementation, configuration and ongoing optimization and support of network components by applying STIGs, IT security principles, network architecture, communication protocols (e.g., TCP/IP), and configuration management. • Conducts secure equipment (e.g., secure telephone and encryption devices) and classified keying material inventories, inspections and other communications security related support and oversight functions • Perform installation of secure telephone equipment and coordinate to deliver encryption device(s) and keying material to select IT specialists maintaining classified networks • Administer a Top Secret inventory and document control program to account for communications security equipment and materials • Conduct inventories per agency policy and reports any discrepancy to government customer • Courier classified information and author receipts for classified materials • Ensure Automated Information Systems Security requirements, related to communications security duties, are complied • Ensure proper physical security accreditation has been issued by designated Program Security Officers for supported facilities • Train personnel in communications security procedures and the use of related equipment	TBD

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
5	Customer Support	Plans and delivers customer support services, including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements. Functions commonly performed include: • Diagnosing and resolving problems in response to customer reported incidents • Researching, evaluating, and providing feedback on problematic trends and patterns in customer support requirements • Developing and maintaining problem tracking and resolution databases • Installing, configuring, troubleshooting, and maintaining customer hardware and software • Developing and managing customer service performance requirements • Developing customer support policies, procedures, and standards • Providing customer training • Ensuring the rigorous application of information security/information assurance policies, principles, and practices in the delivery of customer support services.	• Customer Service and Technical Support (NICE Specialty Area) • Data Administration (NICE Specialty Area) • Education and Training (NICE Specialty Area) • Knowledge Management (NICE Specialty Area) • Network Services (NICE Specialty Area) • System Administration (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Systems Security Analysis (NICE Specialty Area) • Systems Security Architecture (NICE Specialty Area)
6	Cybersecurity Analyst	Monitors security tools for potentially suspicious network traffic, conducts log reviews of security tools, and/or declares incidents. Collects, organizes and interprets data and information to maintain 24/7 operational situational awareness of current and emerging threats. Analyzes network activity for evidence of suspicious behavior to identify and report events that have occurred or might occur within the network. Responds to cybersecurity incidents within the pertinent domain to mitigate immediate and potential threats. Triages, escalates, and/or manages responses to HHS events and incidents; tracks and reports on events/incidents through remediation; and creates matrices for reported incidents and trend analysis. Distributes cyber-related alerts, warnings, and advisories. Participates in Post-Incident Activities/Lessons Learned. Adheres to National Institute of Standards and Technology (NIST800-61 rev 2 and prospective future revisions) guidelines when performing incident-handling, gathering	• Cybersecurity Analysis (Derivative of NICE Specialty Area CND Analysis) • Security Monitoring and Event Analysis (HSAC Task) • Incident Response (NICE Specialty Area) • Exploitation Analysis (NICE Specialty Area) • Network Forensics (Derivative of NICE Specialty Area Digital Forensics) • Security Engineering - Operations (HSAC Task)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	pertinent information regarding events and incidents in real-time. Serves as initial point of contact (POC) for events of interest reported both internally and externally. Consults with investigative/enforcement entities, such as the OIG and United States Computer Emergency Response Team on declared incidents. Follows established NIST and HHS incident escalation processes and coordinates response to computer security incidents. Creates incident tickets, and records all actions taken by HHS Incident Response Teams throughout the incident lifecycle using HHS incident response tracking tools. Initiates and maintains contact with affected parties during incident response lifecycle. Works closely with both internal HHS and external incident response stakeholders to track incidents from initiation through resolution. Follows up on post-incident actions. **NOTE:** In an advanced career level within this role category, a cybersecurity analyst may analyze cyber events and network environments to find trends, patterns, or anomaly correlations that indicate more serious attacks or future threats, and recommend proactive measures to contain computer/network incidents; and isolate and characterize incidents and direct mitigation, preparedness, response, and recovery approaches as needed, to maximize information security; and create and maintain processes and work flows for standard response activities. Due to the federated nature of HHS and its OpDivs, this advanced level of cybersecurity analysis, as it is defined here, may not be vastly present at HHS as it is in other federal departments/agencies, such as the Department of Defense.	

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
7	Cybersecurity Intelligence Analyst	Fuses multiple intelligence disciplines to assess cyber threat capabilities of current and emerging threats to drive insight to inform policymakers/operators. Conducts research and evaluates technical and all-source intelligence to develop in-depth analysis and assessment on threats to systems, critical networks and critical infrastructure. Analyzes technical and intelligence information to provide cyber threat indicators/indications, warnings, and trends. Synthesizes and places intelligence information into context and draws insights about the possible implications. Conducts all-source research to determine adversary capability and intent. Prepares assessments and cyber threat profiles of current events based on collection and research using classified and open source information sources and understanding of the attackers' motivation, language, organization, and social behaviors, thereby helping organizations become more proactive in their security posture and defense. Performs all-source intelligence analyses of cyber activities to identify attributes of interest (their tactics, techniques and procedures [TTPs], motives, and capabilities). Performs post-event analysis, and produces technical intelligence reports for users, senior officials, and other customers and as representative cases. Conducts counterintelligence activities to understand, deter, counter, and mitigate threat activities (e.g., Foreign Intelligence and Security Services (FISS), trans-national organized crime, and insider threat) which exist within the cyber domain and target HHS personnel or information and communications technology networks. Supports all aspects of the intelligence lifecycle (e.g., plan, collect, evaluate, assess, report).	• All Source Intelligence (NICE Specialty Area) • Computer Network Defense Analysis (NICE Specialty Area) • Cyber Operations (NICE Specialty Area) • Cyber Operations Planning (NICE Specialty Area) • Digital Forensics (NICE Specialty Area) • Exploitation Analysis (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Investigation (NICE Specialty Area) • Targets (NICE Specialty Area) • Threat Analysis (NICE Specialty Area)
8	Cybersecurity Research and Forensics Professional (includes Penetration Tester as senior-most career level within this category)	Coordinates Department-wide incident response to: (1) research hackers, hacker techniques, vulnerabilities, and exploits to enhance situational awareness; (2) ensure appropriate investigation, collection, preservation, and analysis of IT security incident-related information and evidence; and (3) report forensic analyses and investigative information, results, and recommendations to the HHS OIS and external entities. Focuses on cyber threat information-	• Vulnerability Assessment and Management (NICE Specialty Area) • Exploitation Analysis (NICE Specialty Area) • Cyber Defense Analysis (NICE Specialty Area) • Digital Forensics (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Threat Analysis (NICE Specialty Area) • Systems Analysis (NICE Specialty Area)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	driven detection, response, and remediation of cybersecurity incidents that affect the Department. May support law enforcement missions by collecting, processing, preserving, analyzing, and presenting computer-related evidence in support of criminal, fraud, or law enforcement investigations. Uses leading technology and industry standard forensic tools and procedures to provide insight into the cause and effect of suspected cyber intrusions, computer incidents and/or crimes. Performs many incident response functions with special emphasis on reverse engineering and malware analysis. Follows proper evidence handling procedures and chain of custody protocols. Produces written reports documenting digital forensic findings, and supplementing mitigation strategies intended to reduce the impact of current and future compromises. Documents activities and findings related to digital media analysis and investigations in final reports. Creates forensically sound duplicates of evidence, and establishes evidence that could potentially be presented in court. May: (1) assess cyber threat capabilities of current and emerging threats to drive insight to inform policymakers/operators; (2) conduct research and evaluate technical and cybersecurity threat information to develop in-depth analysis and assessment on threats to systems, critical networks and critical infrastructure; (3) analyze technical and threat information to provide cyber threat indicators/indications, warnings, and trends; (4) put threat information into context and draw insights about the possible implications; (5) conduct research to determine adversary capability and intent; (6) prepare assessments and cyber threat profiles of current events based on collection and research using classified and open source information sources and understanding of the attackers' motivation, language, organization, social behaviors, and TTPs thereby helping organizations become more proactive in their security posture and defense; and (7) perform post-event analysis, and produce technical threat reports for users, senior officials, and other customers and as representative cases **At most advancing levels** of this role category, follows a systematic methodology to assess, identify and	• Penetration Testing (HSAC Task)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
		demonstrate attack vectors and their impacts to provide risk mitigation/remediation strategies. Maintains knowledge of system architecture designs, current threats and methodologies (TTPs) and security requirements (e.g., NIST, FISMA, etc.) to conduct sophisticated penetration testing throughout the lifecycle. Demonstrates capability in running advanced exploitation techniques with and without the use of automated tools. Performs ongoing vulnerability assessments using commercial and in-house developed tools, reports results to system owners, and tracks vulnerabilities over time. May work with OpDiv POCs on all phases of vulnerability scanning, set up and maintain scheduled scans, review scan results to compile into reports, tune the vulnerability scans to eliminate false positives and streamline the scanning process, identify system vulnerability trends, and update software including the latest signatures.	
9	Data Management Specialist	Plans, develops, implements, and administers systems for the acquisition, storage, and retrieval of data. Functions commonly performed include: • Analyzing and defining data requirements and specifications • Designing, normalizing, developing, installing, and implementing databases • Maintaining, monitoring, performance tuning, backup, and recovery of databases • Installing, configuring, and maintaining database management systems software • Analyzing and planning for anticipated changes in data capacity requirements • Developing and administering data standards, policies, and procedures • Developing and implementing data mining and data warehousing programs • Evaluating and providing recommendations on new database technologies and architectures • Ensuring the rigorous application of information security/ information assurance policies, principles, and practices	• Customer Service and Technical Support (NICE Specialty Area) • Data Administration (NICE Specialty Area) • Knowledge Management (NICE Specialty Area) • Security Engineers/Architects for building security in (HSAC Task) • Software Assurance and Security Engineering (NICE Specialty Area) • System Administration (NICE Specialty Area) • Systems Development (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Systems Security Analysis (NICE Specialty Area) • Systems Security Architecture (NICE Specialty Area) • Technology Research and Development (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	in the delivery of data management services	
10 Information Security Architect (INFOSEC Architect)	Defines and applies industry-standard principles and theories of enterprise architecture throughout the planning, programming, budgeting, and execution (PPBE) cycle. Defines, plans, and applies architectural elements in the analysis, planning, design, implementation, documentation, assessment, and management of the enterprise security architecture. Aligns goals, structure, and processes to IT strategy and agency mission. Ensures secure solutions are incorporated into every aspect of the enterprise architecture supporting an organization's key business processes and organizational mission. Provides the interface between the Enterprise Architect and the Information System Security Engineer. Applies knowledge about current threats to iterative updates of the system architecture. Validates implemented systems against the established architecture. Adjusts designs based on new defense, threat, and attack information. Ensures security components (Security Assessment and Authorization, and infrastructure) are included into new product releases; ensures security (and Plan of Action and Milestones (POA&M) fixes) in new releases and deployment.	• Data Administration (NICE Specialty Area) • Security Program Management (NICE Specialty Area) • Software Assurance and Security Engineering (NICE Specialty Area) • Risk Assessment Engineering (HSAC Task) • Systems Development (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Systems Security Architecture (NICE Specialty Area) • Security Engineering - Architecture for Building Security in (HSAC) • Strategic Planning and Policy Development (NICE Specialty Area) • Technology Demonstration (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area)
11 Information Security Auditor (INFOSEC Auditor)	Oversees, evaluates, and/or supports the documentation, validation, and accreditation processes necessary to assure new IT systems meet the organization's IA requirements and follows a systematic process to assess the ability of systems and networks to withstand sophisticated adversaries who have the knowledge of the architecture and systems deployed. Ensures compliance from internal and external perspectives; conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and	• Information Assurance Compliance (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area) • Vulnerability Assessment and Management (NICE Specialty Area) • Customer Service and Technical Support (NICE Specialty Area) (Note: The competency model definition for this role should focus less on the "helpdesk" concept and more on customer management/relations.)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
		nonoperational situations. Defines and manages IT assessment and accreditation related programs and/or projects, or other area of responsibility, to include strategic direction for system assessment initiatives and activities, personnel, infrastructure, policy enforcement, emergency planning, IT and/or cybersecurity awareness, and/or other resources. Serves as the Point of Contact for elevating unexpected issues that may arise to senior leadership.	
12	Information Security Services (ISS) Information Systems Security Officer (ISSO)	Ensures security requirements and practices are implemented/incorporated throughout the Systems Development Lifecycle (for HHS and the Enterprise Performance Lifecycle) and enables and supports strengthening of HHS' cybersecurity posture. Facilitates protection of HHS systems and the public's personal information to minimize risk to an organization. This includes ensuring compliance with FISMA. Uses NIST and other federal guidelines for security compliance of applications, products, information systems, cloud-based solutions, and network environments. Maintains current knowledge of attack techniques of adversaries and countermeasures against any components being engineered into new or updated systems. Uses knowledge of current attacks to continually identify flaws and weaknesses in the composition and design of networks, remote access schemes, systems, and applications. Translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes. Ensures organizational security requirements in new releases and deployment implemented. Facilitates POA&Ms toward remediation. Oversees and/or authors and maintains security documentation and ensures appropriate controls and documentation for interconnecting systems are in place. Ensures support systems undergo appropriate validation and accreditation processes necessary to assure new and existing IT system(s) meet organizational and federal IA requirements/guidance. Oversees the implementation of IT security controls and ensures systems are compliant with mandated security policies and requirements. Ensures and manages continuous monitoring in accordance with organizational policies. Ensures compliance from internal	• Information Assurance Compliance (NICE Specialty Area) • Information Systems Security Operations (NICE Specialty Area) • Computer Security Infrastructure Support (Derivative of NICE Specialty Area CND Infrastructure Support) • Incident Response (NICE Specialty Area) • Regulatory Requirements and Policy Implementation (derivative of NICE Specialty Area: Legal Advice and Advocacy) • Security Program Management and Customer Service (Combination of NICE Security Program Management and NICE Customer Service) • Security Risk Assessment and Systems Security Analysis (Combination of HSAC Task Risk Assessment Engineering and NICE Specialty Area Systems Security Analysis) • Systems Security Development and Requirements Planning (Derived from NICE Systems Requirements Planning)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	and external perspectives; conducts/reviews risk and vulnerability assessments of threats and vulnerabilities; determines deviations from acceptable configurations and enterprise or local policy; assesses shortcomings related to business requirements and functionality; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations. Coordinates security and compliance assessments, audits, and security testing for system(s). Performs program/project management functions relevant to the security lifecycle of a system(s). Promotes IT security awareness information to the user community. Evaluates security requirements as part of the procurement process. Reviews possible risks introduced by new hardware/software. Oversees and maintains regulatory requirements and participates on the Change Control Board (CCB) by reviewing changes for security implications and any other relevant security deviations. Serves as the POC for elevating system security-related risks and issues that may arise to senior leadership.	
13 Information Security Services (ISS) Systems Security Analyst	Authors and maintains Security Assessment & Authorization (SA&A) Packages required for a system to receive the Authority to Operate (ATO). Ensures support systems undergo the appropriate validation and accreditation processes necessary to assure new and existing IT system(s) meet organizational and federal IA requirements/guidance: • Identifying sources of security requirements, such as relevant laws, regulations, and standard; • Ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements • Outlining initial thoughts on key security milestones including time frames or development triggers that signal a security step is approaching • Making initial delineation of business requirements in terms of confidentiality, integrity, and availability • Determining information categorization and	• Incident Response (NICE Specialty Area) • Information Assurance Compliance (NICE Specialty Area) • Information Systems Security Operations (NICE Specialty Area) • Knowledge Management (NICE Specialty Area) • Regulatory Requirements (derivative of NICE Specialty Area: Legal Advice and Advocacy) • Systems Security Analysis (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area) • Vulnerability Assessment and Management (NICE Specialty Area) • Systems Security Architecture (NICE Specialty Area) – BASIC LEVEL KNOWLEDGE • Software Assurance and Security Engineering (NICE Specialty Area) – BASIC LEVEL KNOWLEDGE • Systems Development (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Technology Research and Development (NICE Specialty Area)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	identification of known special handling requirements to transmit, store, or create information such as personally identifiable information • Determining any privacy requirements. The SA&A Package consists of several documents and test results that provide the foundation of information for a Certifying Authority to make a decision on whether a system receives an ATO and is allowed to start processing federal data. From a high level the SA&A package consists of the following documents: System Security Plan in accordance with NIST 800-53, Revision 4; Configuration Management Plan; Privacy Impact Assessment; Contingency Plan; Contingency Plan Test; Incident Response Plan; Rules of Behavior; Security Controls Assessment; Security Assessment Report; Risk Assessment; POA&M; and Authority to Operate Request Memo. Provides Program Management, Policy, Oversight, and Enterprise Risk Management through the following activities: program management and budget; policy and standards development and management; common controls management and implementation; enterprise contingency planning and testing; enterprise risk management; system authorization; incident response planning; security boundary management; security planning and documentation; control implementation; procedures development and maintenance; POA&M and corrective actions planning; systems contingency planning; and system decommissioning.	• Security Program Management (NICE Specialty Area) • Strategic Planning and Policy Development (NICE Specialty Area)
14 Information Technology Architect (IT Architect)	Plans, designs, implements, documents, assesses, and manages the enterprise structural framework to align IT strategy, plans, and systems with the mission, goals, structure, and processes of the organization. Functions commonly performed include: • Developing reference models of the enterprise and maintaining the information in the IT repository	• Systems Development (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Systems Architecture (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	• Determining the gaps between the current and the target architecture and developing plans for transitioning to target architecture • Defining the policies and principles to guide technology decisions for the enterprise architecture • Identifying opportunities to improve enterprise-level systems to support business processes and utilize emerging technologies • Promoting and educating customers and stakeholders on the use and value of the enterprise architecture • Providing enterprise architecture guidance, support, and coordination to customers and IT project teams • Documenting the enterprise architecture infrastructure, including the business units and key processes, using modeling techniques • Ensuring technical integration is achieved across the enterprise by participating in test planning, validation, and reviews • Evaluating the impact of enterprise architecture products and services on IT investments, business operations, stakeholder satisfaction, and other outcomes • Coordinating and conducting governance and portfolio management activities associated with ensuring compliance with the enterprise architecture • Ensuring the rigorous application of information security/ information assurance policies, principles, and practices to all components of the enterprise architecture	
15 Information Technology Engineer	Plans, installs, configures, tests, implements, and manages the systems environment in support of the organization’s IT architecture and business needs. Functions commonly performed include: • Analyzing systems requirements in response to business requirements, risks, and costs • Evaluating, selecting, verifying, and validating the systems software environment • Evaluating, selecting, and installing compilers, assemblers, and utilities • Integrating hardware and software components within the	• Network Services (NICE Specialty Area) • Risk Management (Derivative of Risk Management NICE Specialty Area and Software Assurance and Risk Assessment Engineering HSAC task) • Security Engineering - Architecture for Building Security (HSAC Task) • Security Engineering Operations (HSAC Task) • System Administration (NICE Specialty Area) • Systems Analysis (NICE Specialty Area) • Systems Architecture (NICE Specialty Area) • Systems Development (NICE Specialty Area)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	systems environment • Monitoring and fine-tuning performance of the systems environment • Evaluating new systems engineering technologies and their effect on the operating environment • Ensuring that information security/information assurance policies, principles, and practices are an integral element of the operating environment	• Systems Requirements Planning (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area) • Vulnerability Assessment and Management (NICE Specialty Area)
16 Information Technology/ Cybersecurity Program & Project Manager	**IT/Cybersecurity Project Coordinator** Ensures that requirements are appropriately written, performance standards are established, and contractor obligations met. Develops requirements, leads integrated project teams (IPTs), and oversees critical budget and governance processes to ensure mission needs are met and expected outcomes are achieved. **IT/Cybersecurity Project Manager** The Project Manager is responsible for directly managing IT projects to provide a unique service or product. They shall develop the business case in conjunction with senior leadership to clearly define and capture business need requirements, conduct project planning (e.g., budgeting, staffing, business management) to adequately define and execute the tasks required to meet approved cost, schedule and performance baselines and conform to HHS policies that apply to IT and/or cybersecurity projects. Project Managers shall be responsible for timely reporting of significant variances from approved baselines and providing corrective action plans or rebaselining proposals as appropriate. Provides oversight to ensure project work is adhering to the larger strategic view developed by senior management at HHS and serves as the POC for elevating unexpected issues that may arise to senior leadership. **IT/Cybersecurity Program Manager** Manages one or more major multi-year IT and/or cybersecurity initiatives that are carried out across HHS OpDivs and through multiple, related IT/cybersecurity projects. Leads, coordinates, communicates, integrates and is accountable for the overall success of the program; ensures alignment with critical agency priorities. Ensures the work efforts achieved are within the agency's business	Note: Because of FITARA PM Competencies focus on FAC-P/PM Competencies • Requirements Development and Management Processes (Aligns with NICE Specialty Area for Systems Requirements Planning) • Systems Engineering • Systems Testing and Evaluation • Lifecycle Logistics • Contracting Business, Cost, and Financial Management • Leadership FAC P/PM IT Core Plus Competencies Accessibility • Configuration Management (Aligns with NICE Systems Requirements Planning) • Data Management • Enterprise Architecture (Aligns with NICE Systems Security Architecture) • Information Assurance (Aligns with NICE IA Compliance) • Information Management (Aligns with NICE Knowledge Management) • Information Resources Strategy and Planning (Aligns with NICE Strategic Planning and Policy Development) • Information Systems Security Certification (Aligns with NICE Systems Security Analysis and CND Infrastructure Support) • Information Systems/Network Security (Aligns with NICE Network Services) • IT Architecture (Aligns with NICE Systems Security Architecture and Test and Evaluation • IT Performance Assessment (Aligns with NICE Technology

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
		strategy, including appropriate strategic, lifecycle management; and capital IT/cybersecurity investment plans. The Program Manager is also responsible for staffing plans, business management, and budgeting; for project selection, prioritization, evaluation and monitoring, cost schedule management, risk management, quality management, and resource allocations.	Research and Development • IT Program Management (Aligns with NICE Security Program Management) • Infrastructure Design (Aligns with NICE Systems Evaluation) • Operations Support (Aligns with Nice Customer Service/Technical Support)
17	Information Technology/ Cybersecurity Training, Outreach, and Awareness Professional	Focuses on content development, communications, and/or training program management in support of IT and cybersecurity awareness or relevant technical subject domains. Coordinates with all IT and cybersecurity programs at HHS, marketing their programs and capabilities across all modal representatives to support IT and/or cybersecurity awareness initiatives. May conduct and/or coordinate training of personnel within pertinent IT and/or cybersecurity subject domain and develop, plan, coordinate, and evaluate training courses, methods, and techniques as appropriate. May be responsible for raising security awareness and facilitating improved security. May participate in the cross-modal IT and/or cybersecurity exercise projects (e.g., planning and coordinating private sector participation, and developing goals and scenarios).	• Strategic Planning and Policy Development (NICE Specialty Area) • Security Program Management (NICE Specialty Area) • Education and Training (NICE Specialty Area) • Customer Service and Technical Support (NICE Specialty Area) (Note: The competency model definition for this role should focus less on the "helpdesk" concept and more on customer management/relations.) • Cybersecurity Workforce Development and Planning (Neither NICE or HSAC capability) • Knowledge Management (NICE Specialty Area) • Information Assurance Compliance (NICE Specialty Area)
18	Information Technology/ Cybersecurity Workforce Development/ Planning Specialist	Aligns the IT and/or cybersecurity needs and priorities of the organization to strategic and operational workforce planning and talent management efforts. Establishes and builds an IT and/or cyber workforce employee pipeline for the future through implementation and continuous improvement of best practices in identifying, acquiring, growing, and sustaining both entry-level and experienced IT and/or cybersecurity technical experts. Identifies parameters for building an effective, mission-focused IT and/or cybersecurity workforce and improving IT and/or cybersecurity practices through recruiting, developing, engaging and retaining IT/cyber staff. Develops individual and organizational capabilities and provides direction, leadership, and guidance on IT/cyber workforce organization structure, resources, staffing, workforce analytics and planning. Identifies standards and guidelines, educational and training certifications, and accreditations,	• Strategic Planning and Policy Development (NICE Specialty Area) • Education and Training (NICE Specialty Area) • Security Program Management (NICE Specialty Area) • Customer Service and Technical Support (NICE Specialty Area) (Note: The competency model definition for this role should focus less on the "helpdesk" concept and more on customer management/relations.) • Cybersecurity Workforce Development & Planning

HHS IT/Cybersecurity Work Role		Work Role Definition	Technical Competencies (NICE Specialty Areas)
		and establishes policies, and human capital management strategies that align with IT/cyber workforce missions, enabling the organization to identify, acquire, grow, and sustain a capable IT/cyber workforce. Supports efforts to create a safe, secure, and resilient IT and/or cybersecurity environment.	
19	IT/Cybersecurity Risk Manager	Conducts strategic assessment of organizational risk posture based on combined analyses of: (a) aggregate risk to HHS and (b) the use of HHS systems. Leads and/or supports the implementation of comprehensive risk management strategies aligned with HHS' risk posture, inclusive of specific programs to include: continuous monitoring, security data analysis, and HHS Federal Risk Authorization Management Program cloud sponsorships. Collaborates with HHS StaffDivs and OpDivs to ensure risk-related information and decisions are made with consideration to StaffDiv/OpDiv and HHS-specific strategic goals and objectives, core missions, and business functions, and acceptable risk posture (i.e., collaborates with OpDivs and StaffDiv personnel to enhance enterprise-wide capabilities to effectively manage information system-related security risks). Works with HHS OpDivs and StaffDivs to ensure risks are managed consistently across the Department to reflect HHS risk tolerance and ensure mission/business success. Facilitates enterprise-level, risk-based decision making and sets the vision and direction for the Risk Management Program and risk management strategies for HHS. Develops performance metrics to establish critical risk and security requirements, identify quantifiable outputs, and establish goals that enable effective measurement. Serves as an advocate for all disciplines within the security program including the development and subsequent enforcement of the agency's security awareness programs, business continuity and disaster recovery plans, and all industry and governmental compliance issues. Supports continuous monitoring through scheduled audits, controls testing, and audit reviews, and escalates issues as needed. Works to ensure the implementation of IT security controls and security authorization documents. Provides technical	• Information Systems Security Operations (NICE Specialty Area) • System Administration (NICE Specialty Area) • Systems Development (NICE Specialty Area) • Systems Security Analysis (NICE Specialty Area) • Systems Security Architecture (NICE Specialty Area) • Information Assurance Compliance (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Customer Service and Technical Support (NICE Specialty Area) (Note: The competency model definition for this role should focus less on the "helpdesk" concept and more on customer management/relations) • Cyber Operations Planning (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Security Program Management (NICE Specialty Area) • Strategic Planning and Policy Development (NICE Specialty Area) • Vulnerability Assessment and Management (NICE Specialty Area) • Risk Assessment Engineering (HSAC Task)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	recommendations for all enterprise Risk Assessments and Vulnerability Assessments conducted across the Department. Oversees and/or maintains regulatory requirements and participates on the CCB by reviewing changes for enterprise risk and vulnerability.	
20 Network Administrator/ Network Engineer	**Network Administrators** Installs, configures, troubleshoots, and maintains network and security devices such as switches, multiplexers, routers, cables, proxies, and secure communications circuits to ensure their confidentiality, integrity, and availability. Responsible for access control, passwords, account creation and administration. Develops and documents network administration standard operating procedures; resolves hardware/software interface and interoperability problems. Ensures network security (confidentiality, integrity, availability), and efficiency; maintains network configuration; manages the installation and integration of network device patches, updates, and enhancements. **Network Engineers** Installs, configures, troubleshoots, and maintains network and security devices such as switches, multiplexers, routers, cables, proxies, and secure communications circuits to ensure their confidentiality, integrity, and availability. Responsible for access control, passwords, account creation and administration. Develops and documents network administration standard operating procedures; resolves hardware/software interface and interoperability problems. Ensures network security (confidentiality, integrity, availability), and efficiency; maintains network configuration; manages the installation and integration of network device patches, updates, and enhancements. Evaluates functional requirements and develops customer-oriented solutions; tests systems to ensure compliance with specifications and requirements. Conducts network health assessments, monitors and uses defensive measures on the network to remediate unauthorized activities, and responds	• Customer Service and Technical Support (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Network Services (NICE Specialty Area) • Security Engineering Operations (HSAC Task) • System Administration (NICE Specialty Area) • Systems Analysis (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area **Additional Competencies for Engineer:** • Cybersecurity Defense Infrastructure Support (NICE Specialty Area) • Risk Management (Derivative of Risk Management NICE Specialty Area and Software Assurance and Risk Assessment Engineering HSAC task) • Security Engineering - Architecture for Building Security (HSAC Task) • Systems Development (NICE Specialty Area) • Vulnerability Assessment and Management (NICE Specialty Area)

HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
	to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.	
21 Research & Development Specialist	Advances the future state of cybersecurity through research and development (R&D) and/or standards (this may include interfacing with public and private sector organizations). Communicates IT/cybersecurity R&D requirements to stakeholders to incorporate research products into mission areas. Influences the development of voluntary consensus of cybersecurity standards to align and improve critical security interests (e.g., interagency interoperability). Facilitates information exchange and supports cybersecurity initiatives. Assists in requirements development and acquisition support for investments of security solutions, technologies, and processes. Identifies, enhances, proliferates, and nurtures adoption of innovative and effective security solutions that address emerging threats. Captures requirements for new and continuous process improvements, determines feasibility of solution implementations, and prioritizes related projects and initiatives. Analyzes current security architectures within the OpDivs and across the HHS enterprise; identifies current attack vectors; identifies unprotected attack surfaces; evaluates and implements incident response and management tools; and assists in security solution implementation projects. Affects numerous high-visibility, high-stakes programs of HHS that are of national and potentially international interest.	TBD

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
22	Risk & Vulnerability Specialist	Develops estimates of risks associated with technologies and discovered threats, enabling organization to assess the resources needed to respond effectively. Follows systematic process to assess the ability of systems and networks to withstand exploitation by adversaries. Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in all situations. Applies the Risk Management Framework to continuously monitor and assesse systems security posture to maintain accurate, near-to-real time picture of security posture, provide visibility into assets, and leverage automated data feeds to quantify risk, ensure effectiveness of security controls, implement prioritized remediation, and determine acceptable risk to security, data, network(s) end points, and cloud devices/applications. Supports OpDivs/StaffDivs in expanding their diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts. May test applications throughout its lifecycle to identify weaknesses. May perform technical tests, network scans, vulnerability scans, and/or penetration testing to evaluate the effectiveness of systems, devices, procedures, and methods used to safeguard information in computer accessible media.	• All Source Intelligence (remove "intelligence community" from the definition) (NICE Specialty Area) • Information Assurance Compliance (NICE Specialty Area) • Security Program Management (NICE Specialty Area) • Strategic Planning and Policy Development (NICE Specialty Area) • Risk Assessment Engineering (HSAC Task) • Systems Requirements Planning (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area) • Exploitation Analysis (NICE Specialty Area) • Vulnerability Assessment and Management (NICE Specialty Area) • Computer Network Defense (CND) • Computer Network Defense Infrastructure Support (NICE Specialty Area)
23	Secure Software Assessor	Ensures secure coding practices are implemented during development and recommends remediation to existing systems. Ensures coding is free of known coding flaws and weak design approaches, and checks software to identify flaws. Recognizes security vulnerabilities in programs while under time, quality, or cost pressures/constraints. Addresses means to reduce exploitable software weaknesses and improve capabilities to routinely develop, acquire, and deploy resilient software products. Enables software security automation and measurement capabilities through use of common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, structured threat information, cyber	TBD

HHS IT/Cybersecurity Work Role		Work Role Definition	Technical Competencies (NICE Specialty Areas)
		observables, and common attacks which target software; enhances software transparency and security diagnostic and measurement capabilities.	
24	Strategic Planning, Policy, and Compliance Professional - Cybersecurity Strategic Planning, Policy, and Compliance Professional	**Cybersecurity Strategic Planning, Policy, and Compliance Professional** Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that support new initiatives or required changes/enhancements that coincide with larger agency mission and/or business goals and objectives. Ensures rigorous application of information security/information assurance policies, principles, and practices. Develops contextual workforce training and education courses of enterprise level requirements. Conducts FISMA compliance reviews and audits. Collects, aggregates, prepares, and submits quarterly and annual FISMA Reports. Coordinates submission of FISMA metrics to higher authority. Distributes FISMA reporting data calls to Operational Divisions. Assists in explaining FISMA reporting requirements.	• Information Assurance Compliance (NICE Specialty Area) • Regulatory Requirements (derivative of NICE Specialty Area: Legal Advice and Advocacy) • Security Program Management (NICE Specialty Area) • Strategic Planning and Policy Development (NICE Specialty Area) • Information Systems Security Management (NICE Specialty Area)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
25	Strategic Planning, Policy, and Compliance Professional - Information Technology Strategic Planning, Policy, and Compliance Professional	**IT Strategic Planning, Policy, and Compliance Professional** Provides a wide range of IT management activities that typically extend and apply to an entire organization or major components of an organization. This includes strategic planning, capital planning and investment control, workforce planning, policy and standards development, resource management, knowledge management, auditing, and information security management. Functions commonly performed include: • Developing and maintaining strategic plans • Assessing policy needs and developing policies to govern IT activities • Providing policy guidance to IT management, staff, and customers • Defining current and future business environments; • Preparing IT budgets • Managing IT investment portfolios • Establishing metrics to measure and evaluate systems performance and total cost of ownership • Identifying and addressing IT workforce planning and management issues, such as recruitment, retention, and training • Conducting audits of IT programs and projects; and/or • Ensuring the rigorous application of information security/ information assurance policies, principles, and practices in the delivery of planning and management services	• Information Assurance Compliance (NICE Specialty Area) • Regulatory Requirements (derivative of NICE Specialty Area: Legal Advice and Advocacy) • Security Program Management (NICE Specialty Area) • Strategic Planning and Policy Development (NICE Specialty Area) • Information Systems Security Management (NICE Specialty Area)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
26	Strategic Planning, Policy, and Compliance Professional - Privacy Professional	**Privacy Professional** Develops, manages, and/or leads development of HHS IT privacy security policy; evaluates automated systems to determine whether privacy is adequately protected; provides guidance to OpDivs for preparing privacy impact assessments; and develops and maintains a Privacy Program strategic plan, agency IT policies, and procedures. Develops and monitors privacy policy and guidelines for Department-wide application to ensure significant Privacy Act issues are addressed. Recommends new and/or changes to Privacy Act processes and systems. Develops, implements and/or leads implementation of policies and programs required by law to ensure the privacy of personal records under the Privacy Act. Serves as an agency subject matter expert (SME) on the HHS-OCIO Policy for Information Systems Security and Privacy. Ensures HHS policies support compliance with the FISMA. Coordinates necessary HHS efforts to comply with the OMB reporting regulations for FISMA and Agency Privacy Management requirements for annual review of the certification and accreditation status of contractor and government systems. Collaborates with other OCIO leaders and/or colleagues to develop and/or implement programs that ensure users understand and adhere to privacy policies and procedures and develops and/or applies methods of reporting and correcting discrepancies.	• Information Assurance Compliance (NICE Specialty Area) • Knowledge Management (NICE Specialty Area) • Security Program Management (NICE Specialty Area) • Education and Training (NICE Specialty Area) • Strategic Planning and Policy Development (NICE Specialty Area) • Regulatory Requirements (derivative of NICE Specialty Area: Legal Advice and Advocacy) • Information Systems Security Management (NICE Specialty Area)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
27	Systems Administrator/Engineer	**Systems Administrator** Installs, configures, troubleshoots, and maintains server/appliance configurations (hardware and/or software) to ensure their confidentiality, integrity, and availability. Responsible for access control, passwords, account creation and administration. Develops and documents systems administration standard operating procedures; resolves hardware/software interface and interoperability problems. Ensures systems security (confidentiality, integrity, availability), and efficiency; maintains systems configuration; manages the installation and integration of system patches, updates, and enhancements. **Systems Engineer** Installs, configures, troubleshoots, and maintains server/appliance configurations (hardware and/or software) to ensure their confidentiality, integrity, and availability. Responsible for access control, passwords, account creation and administration. Develops and documents systems administration standard operating procedures; resolves hardware/software interface and interoperability problems. Ensures systems security (confidentiality, integrity, availability), and efficiency; maintains systems configuration; manages the installation and integration of system patches, updates, and enhancements. Evaluates functional requirements and develops customer-oriented solutions; tests systems to ensure compliance with specifications and requirements. Conducts system health assessments, monitors and uses defensive measures on the system to remediate unauthorized activities, and responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.	• Customer Service and Technical Support (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Network Services (NICE Specialty Area) • Security Engineering Operations (HSAC Task) • System Administration (NICE Specialty Area) • Systems Analysis (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area) **Additional Competencies for Engineer:** • Cybersecurity Defense Infrastructure Support (NICE Specialty Area) • Risk Management (Derivative of Risk Management NICE Specialty Area and Software Assurance and Risk Assessment Engineering HSAC task) • Security Engineering - Architecture for Building Security (HSAC Task) • Systems Development (NICE Specialty Area) • Vulnerability Assessment and Management (NICE Specialty Area)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
28	Systems Analyst	Applies analytical processes to the planning, design, and implementation of new and improved information systems to meet the business requirements of customer organizations. Functions commonly performed include: • Performing needs analyses to define opportunities for new or improved business process solutions • Consulting with customers to identify and specify requirements • Developing overall functional and systems requirements and specifications • Conducting business process reengineering; • Conducting feasibility studies and trade-off analyses • Preparing business cases for the application of IT solutions • Defining systems scope and objectives • Developing cost estimates for new or modified systems • Ensuring the integration of all systems components; e.g., procedures, databases, policies, software, and hardware • Planning systems implementation • Ensuring the rigorous application of information security/ information assurance policies, principles, and practices to the systems analysis process	• Risk Assessment Engineer (HSAC Task) • Secure Coders and Code Reviewers (HSAC Task) • Security Engineers - Operations (HSAC Task) • Security Engineers/Architects for building security in (HSAC Task) • Software Assurance and Security Engineering (NICE Specialty Area) • System Administration (NICE Specialty Area) • System and Network Penetration Tester (HSAC Task) • Systems Development (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Systems Security Analysis (NICE Specialty Area) • Systems Security Architecture (NICE Specialty Area) • Technology Research and Development (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area)

	HHS IT/Cybersecurity Work Role	Work Role Definition	Technical Competencies (NICE Specialty Areas)
29	Systems Security Subject Matter Expert (SME) (Previously titled "Information Systems Security Engineer (ISSE)")	**Systems Security Subject Matter Expert (SME)** (Previously titled "Information Systems Security Engineer (ISSE)") Act as subject matter expert for one or more information security systems. Ensures implementation of security requirements and security practices are incorporated throughout the system engineering lifecycle and engineering maintenance of solutions, applications, products, information systems, and network environments to minimize risk to the organization. Maintains currency on attack techniques being used by adversaries and countermeasures against any supported systems. Implements and configures information security systems at the highest appropriate level of security. Uses knowledge about current threats to develop remediation, mitigation, and monitoring plans to protect information systems and data. Translates business requirements, technology, and environmental conditions (e.g., law and regulation) into system and security designs and processes. Assesses systems for shortcomings related to business requirements, functionality, or policy compliance and develops and documents steps to mitigate. Evaluates functional requirements and develops customer-oriented solutions.	• Customer Service and Technical Support (NICE Specialty Area) • Cybersecurity Defense Infrastructure Support (NICE Specialty Area) • Incident Response (NICE Specialty Area) • Network Services (NICE Specialty Area) • Risk Management (Derivative of Risk Management NICE Specialty Area and Software Assurance and Risk Assessment Engineering HSAC task) • Security Engineering - Architecture for Building Security (HSAC Task) • Security Engineering Operations (HSAC Task) • System Administration (NICE Specialty Area) • Systems Analysis (NICE Specialty Area) • Systems Architecture (NICE Specialty Area) • Systems Development (NICE Specialty Area) • Systems Requirements Planning (NICE Specialty Area) • Test and Evaluation (NICE Specialty Area) • Vulnerability Assessment and Management (NICE Specialty Area)