



To Infinity & Beyond

Operationalizing the NICE Framework for
Career Profiles

Joshua Musicante

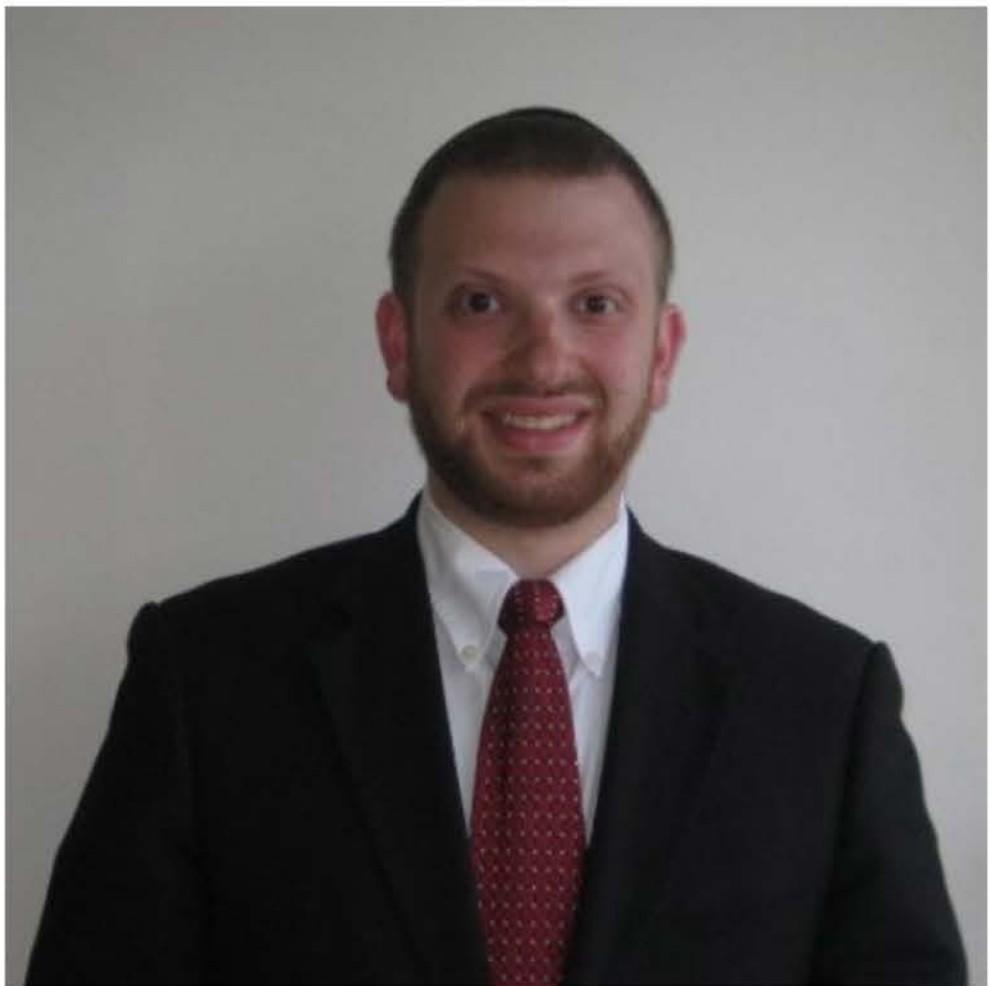
Lead, IT & Cybersecurity Workforce Analytics



@joshuamusicante



[linkedin.com/in/joshua-musicante-3292ba1b/](https://www.linkedin.com/in/joshua-musicante-3292ba1b/)



About Josh

Josh Musicante is a leader in strategic workforce planning and development, human capital management, and workforce analytics. He has supported multiple organizational human capital-related efforts for the cybersecurity workforce. At HHS, Josh leads workforce analytics initiatives for the IT and cybersecurity workforce.

Sarah Moffat

HHS Enterprise Lead
IT/Cybersecurity Education &
Professional Development



@sarahcmoffat



@sarahdipity40



Linkedin.com/sarahcmoffat

My Personal Mission Statement

To create an open space where all feel welcomed, safe, empowered, and treasured (valuable). To be creative and inspired – as God made me – and inspire others to find their own voice and creativity, to pursue their passions, and to build a life and career that matters to them. To embolden others to discover their “why”, and help them develop the knowledge, skills, and attitudes to actively fulfill their own personal mission.

Who I Am

- Creative
- Helpful
- Energetic
- Strategic Visionary
- Ambitious
- Driven
- Hilarious
- Geniune
- Curious
- Life-long Learner
- Engaging
- Empowering



AGENDA



Introduction



The Problem



Government Solutions



Where HHS Has Been (To Infinity)



Where HHS is Going (Beyond)

01

The Problem



LESS MONEY & MO' PROBLEMS



02

The Government's Solutions



LEGISLATIVE & POLICY SOLUTIONS

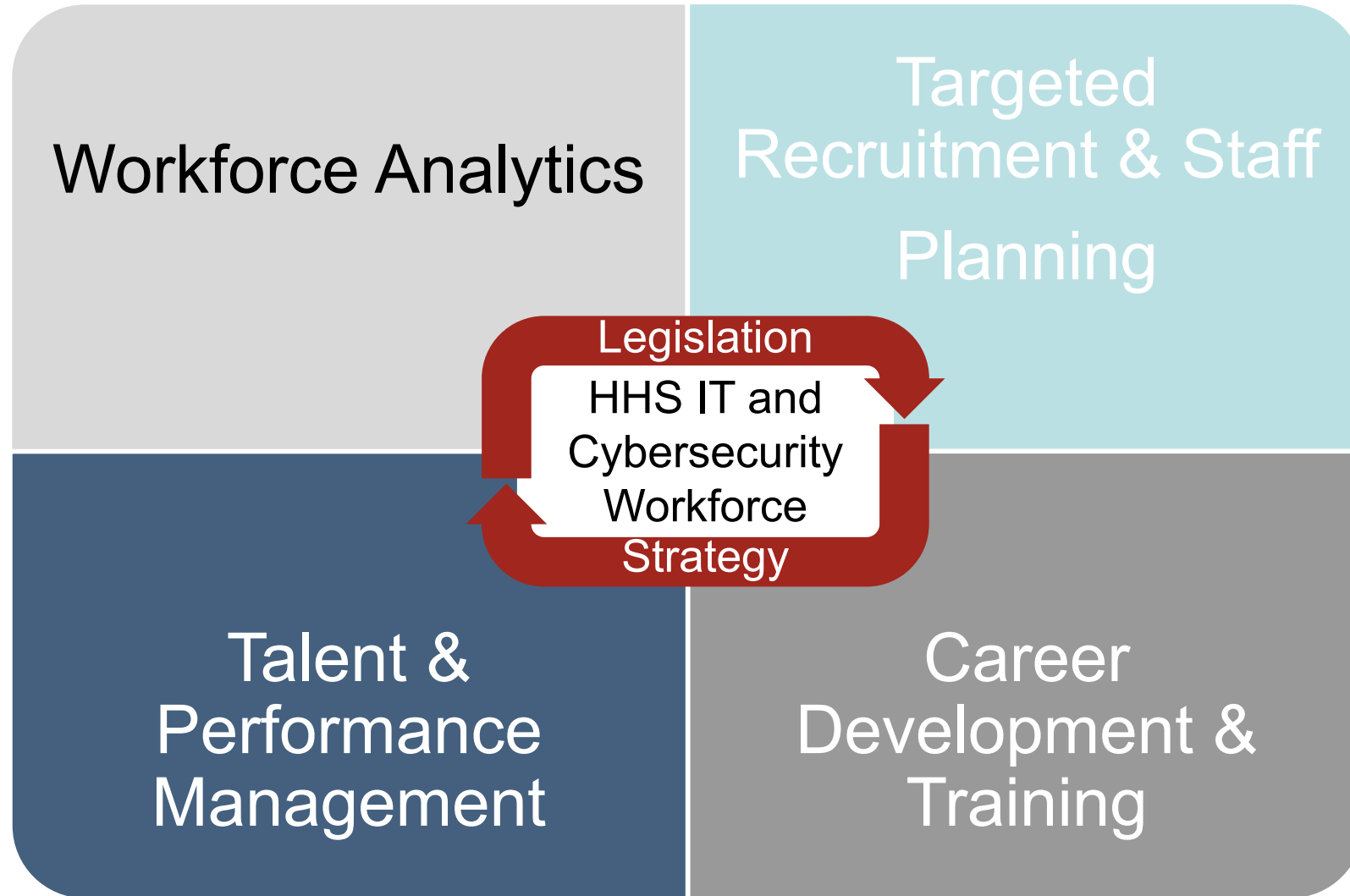


03

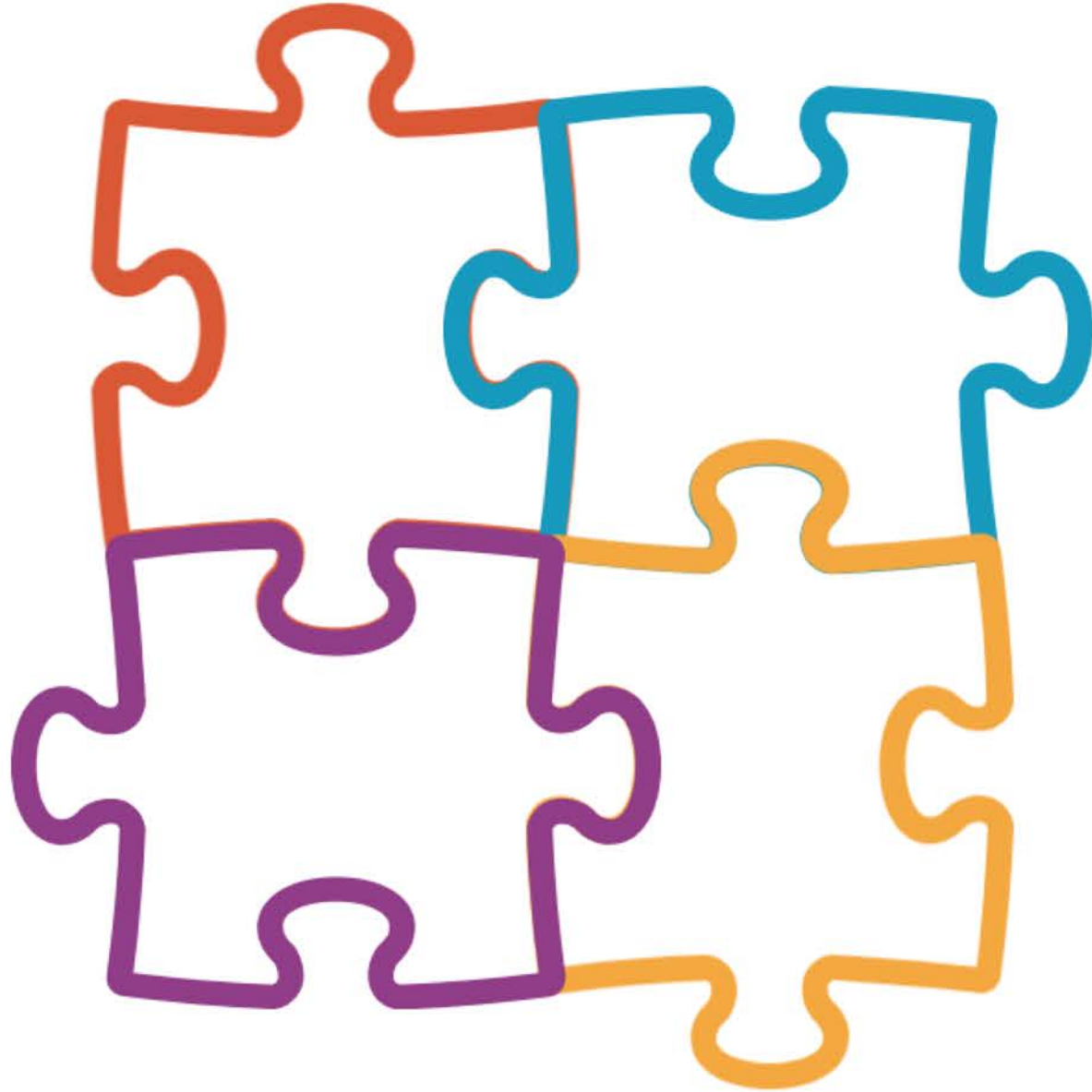


What HHS has Done (to infinity)

IT & CYBERSECURITY WORKING GROUP



CAREER PATH & COMPETENCY MODELS

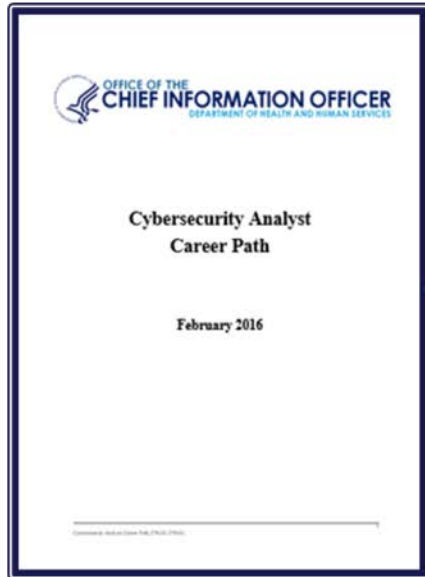


Specialty Areas →
Competencies

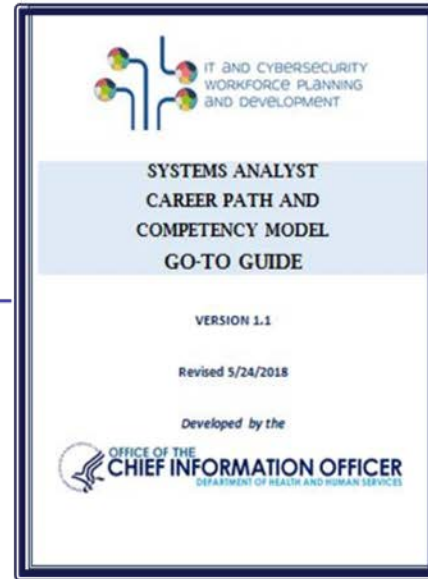
Technical Focus

Competency-Based
Development

Career Path



Go-To Guide



Professional Profile

- The Career Paths (+/- 85 pages) have been condensed into summarized versions:
 - Career Path Go-To Guide (~20 pages)
 - Professional profile (~2 pages)
- Designed to:
 - Be user friendly
 - Support Professional Development
 - Compliment SharePoint Career Path Tool
 - Support OPM and GAO Data Calls

RESEARCH AND DEVELOPMENT SPECIALIST PROFESSIONAL PROFILE

This professional profile quick sheet provide a small snapshot of the career path and required competencies for the Research and Development Specialist work role in the Department of Health and Human Services. There are more resources about your professional profile including a full competency model and career path, a key differentiators tool that you can use to help you chart your skills from one level of proficiency to the next. To see the full catalog of available resources for the Research and Development Specialist Work Role, please email TheMightyIT@hhs.gov for access to our IT and Cybersecurity Workforce Development website.

Your Role Definition

Advances the future state of IT/cybersecurity through research and development (R&D) and industry standards. Identifies emerging IT trends by engaging public and private sector organizations such as academia, health care, and venture capitalists. Communicates IT/cybersecurity research and findings to stakeholders to support mission areas. Builds consensus to align and improve mission execution through interagency operability, solution standardization, and cost savings. Directs requirements development and supports acquisition of security solutions, technologies, and processes. Identifies, enhances, proliferates, and nurtures adoption of innovative and effective technologies that address emerging threats. Captures requirements for new and continuous process improvements, determines feasibility of solution implementations, and prioritizes and pilots related projects and initiatives. Analyzes current security architectures within the OpDivs and across the HHS enterprise and engages senior leadership to identify existing gaps and future priorities. Affects high-visibility investments with significant impact to HHS.

Your Job Title Might Be

- Cybersecurity R&D Professional
- Cybersecurity Standards Professional
- R&D Engineer
- R&D Technician
- R&D Senior Technician
- Computer Systems Analyst
- Computer and Information Research Scientist
- Information Security Analyst
- Security Architect
- R&D Project Manager
- Senior Technologist

Top 10 Preferred Certifications

1. SEI Certificate in Information Security
2. CompTIA (Security+, Cloud+)
3. EC Council (CEH, CIFI)
4. GIAC (GCIA, GXP, GSE)
5. ISC² (CCFP, CISSP, CAP, CCSP)
6. ISFCE
7. CCE
8. Cisco (CCNP, CCNA)
9. Certified Change Management Practitioner
10. ITIL Foundations

Key Learning Opportunities:

- Black Hat Conference
- SANS Institute conferences
- ISC² Conference

Key Development Opportunities:

- Job rotations
- Excellence in Government
- Interagency Tiger Teams/Working Groups
- CIO/CISO Council
- Toastmasters

Your Required Technical Competencies

Competency	Definition
IT/Cyber Leadership	Assesses/leads and/or manages IT/cyber-related work and operations. Applies, evaluates/assesses, and supports information security within the organization, specific program, or other areas of responsibility.
Program/Project Management and Acquisition	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage IT/cybersecurity programs. Provides direct support for the use of information technology (IT) applying IT-related laws and policies, and provides IT-related guidance throughout systems/program lifecycle.
Risk Management	Analyzes an organization's current computer systems and procedures to evaluate and support the organization's IT/cybersecurity, risk and compliance requirements to align with agency risk tolerance/thresholds.
Strategic Planning and Policy	Develops policies and plans and/or advocates for changes in policy that supports organizational IT/cybersecurity initiatives.
Systems Architecture	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
Systems Requirements Planning	Consults with stakeholders to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to meet business needs.
Technology Research and Development	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

Your Potential Career Path



Research & Development Specialist



CERTIFICATION ALIGNMENT & NO-COST TRAINING



Mapping of Certifications to NICE Framework

This certification mapping matrix was built on the work developed by the Health and Human Services...Office of the Chief Information Officer (OCIO) with feedback provided by the HHS OpDivs and StaffDivs.

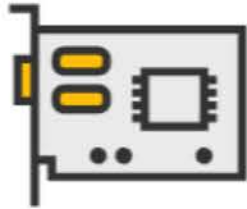


04

Where HHS is Going (and beyond)

WHOLE PERSON DEVELOPMENT

WE ARE TECHNICAL, BUT WE ARE PEOPLE



TECHNICAL COMPETENCIES

Analyze, Recruit, Train, Retain
Technical Workforce



LEADERSHIP COMPETENCIES

If we develop a technical staff
without developing leadership
qualities, we're only developing half of
the person.



TECHNICAL CAREER PATH

Equip workforce with career mobility
and a path forward (Retain &
Develop)



'SOFT SKILLS'

72% of execs said the need for soft skills in
cybersecurity have increase.

PARTNERS IN EXCELLENCE **REVOLUTION**



**Performance
& Development**



Job Rotations



**Modern
Mentoring**



**Learning &
Networking**

This is where I want to go

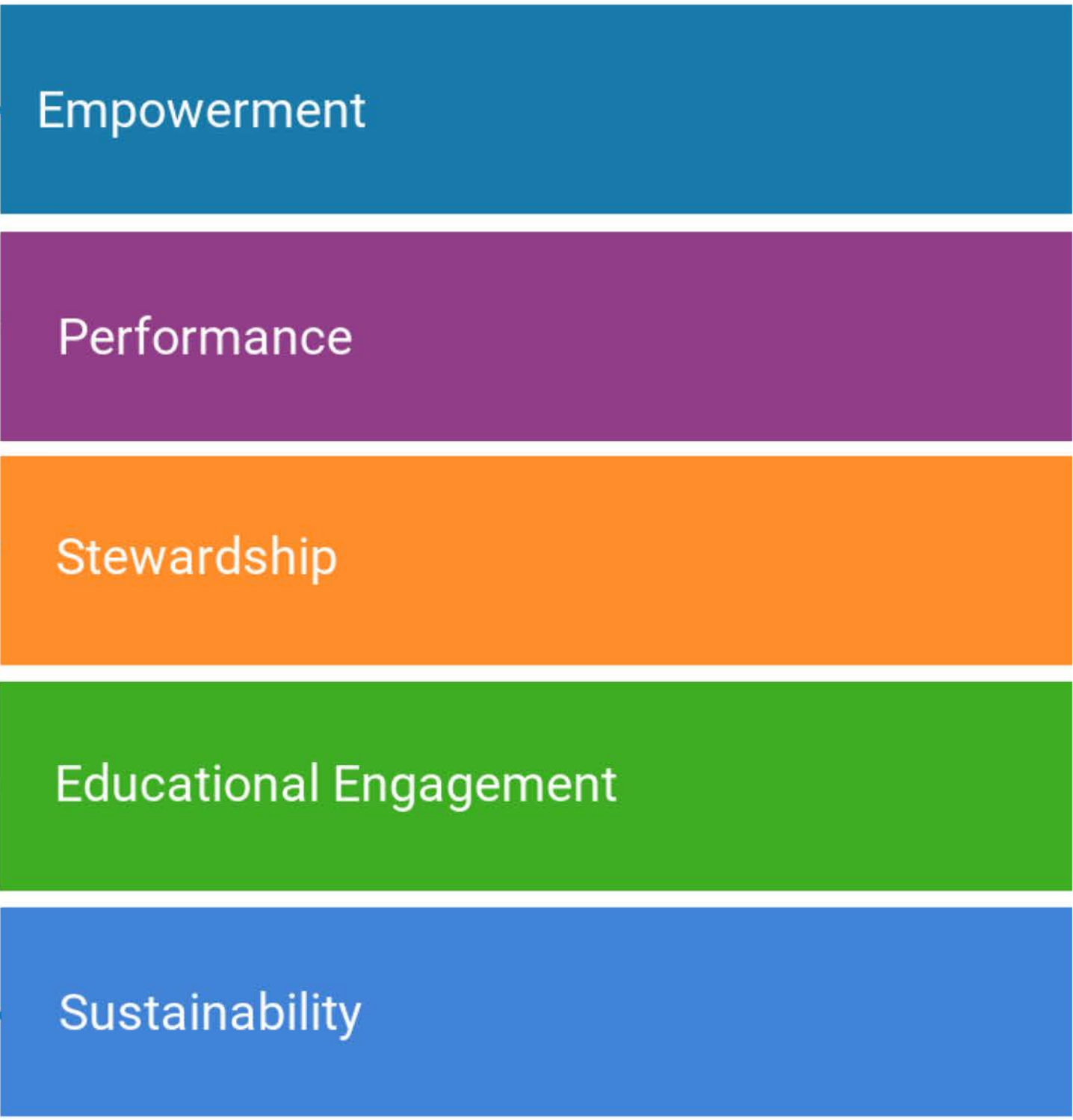


This is how I'll get there...



Partners in Excellence Revolution

PIER



Empowerment

Performance

Stewardship

Educational Engagement

Sustainability

HHS IT & CYBERSECURITY CAREER DEVELOPMENT SITE

Site Navigation

[Career Development](#)

[PIER](#)

[Catalog of Free Technical Training](#)

[Link to LMS](#)

[Link To External](#)

- [Programs for Veterans](#)
- [FedVTE](#)
- [FedCTE](#)
- [SNHU – Discounts for Feds](#)
- [Cybrary](#)
- [Coursera](#)
- [Safari](#)
- [Point3](#)

[Performance Standards Dictionary](#)

[PMAP Training Online](#)

[Meet a Mentor](#)

Page Intro...

Intro page that uses plain language to describe the site and the contents. This will be followed by a description of the site navigation tree to the left of this section.

Professional Profile of the Month

Cybersecurity Analyst

HHS Cybersecurity Analysts make up XX% of our IT and Cybersecurity population. They're responsible for collecting, organizing, and interpreting data to maintain full operational and situational awareness of current and emerging threats. Some preferred certifications include COMPTIA A+, Network+, and Sec+. Analysis, Network Forensics, and Incident Response are a few of the technical competencies required in this job. Click here to learn more...

Professional Profile of the Month

News...

Add some news here. What's happening? Did someone win an award? Is there a new cert in the news? What about a new threat? That would all go here in snippets which would link to a full new page...

Upcoming Conferences & Learning Opps

This section will promote upcoming conferences and professional development opportunities relevant to the Workforce. It will be split into 3 sections.

Build Your Technical Muscle

Classes for technical things...

- BLACK HAT
- PMP class
- FAC P/PM Class
- CISSP
- Sec+



*Click any link to
register or learn
more!*

Develop your Leadership Skills

Including activities that align to Building Coalitions and Leading People:

- PIER Networking Event
- PIER Leadership Development Meeting
- Meeting of Privacy Professional Club
- Risk Management Forum

Experiential Learning

- Capture the Flag
- Bug Bounty
- Whatever

CAREER DEVELOPMENT



Application
Software
Specialist



Chief
Information
Officer



Chief
Information
Security
Officer



COMSEC
Manager



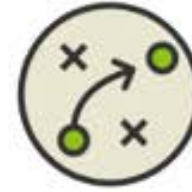
Cybersecurity
Analyst



INFOSEC
Architect



ISS Sys Sec
Analyst /
Systems
Analyst



Strategic
Planning,
Policy,
Compliance



Training,
Outreach, and
Awareness
Professional



Data
Management
Specialist



Forensics
Professional



INFOSEC
Auditor



ISSE / Systems
Security SME



ISSO



Information
Technology
Engineer



Network
Admin /
Engineer



Privacy
Professional/
Privacy
Compliance
Manager



System
Admin/
Engineer



Project/
Program
Manager



Data
Management
Specialist



IT and
Cybersecurity
Customer
Support



Workforce
Development
and Planning



IT Architect /
IT Engineer



Secure
Software
Assessor



IT Portfolio
Manager

Cybersecurity Analyst Profile

Role description...

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. Responds to cybersecurity incidents within the pertinent domain to mitigate immediate and potential threats. Distributes cyber-related alerts, warnings, and advisories. Participates in Post-Incident Activities/Lessons Learned. 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 IRTs throughout

General Staff Levels: GS 9 – 15

Click a career-level to see the Technical Competency Profile for that level

GS 9-11: Junior

GS 12-13: Mid-Level

GS 14-15 Senior

SES, SL, ST: Executive

Relevant Technical Competency Profile

These technical competencies align to the NICE Framework* and represent the technical make-up for Cybersecurity Analyst. Hover your mouse over each competency to see a brief definition related to cybersecurity analysis. Click the competency to see a list of behaviors and performance standards.

Cybersecurity Analysis	Security Monitoring and Event Analysis
Exploitation Analysis	Incident Response
Network Forensics	Security Engineering Operations

HHS Competencies

Click a competency below to read more about it in HHS' PMAP Reference Guide. The PMAP reference guide provides guidance about how to identify and document SMART goals in your annual performance management appraisal. As you are developing your PMAP performance standards, this list of competencies may help by adding measurable performance objectives in these core categories.

External Awareness	Accountability
Flexibility	Decisiveness
Resilience	Customer Service
Problem Solving	Partnering

Conference and Learning Experiences

Click a link below to learn more...

- Any GIAC certification
- BlackHat Conference (recommended for Tier 3 Analysts)
- BSides Security Conferences (recommended for all Analysts)
- Business writing/communication (recommended for all levels of Analyst)
- CEH Certification (recommended for Analysts for Analysts Tiers 1-3)
- CEH Certification (recommended for Analysts Tiers 1-3)
- CISSP (recommended for Analysts Tiers 2-3)
- CISSP Certification (recommended for Analysts Tiers 2-3)
- Code Academy training modules (recommended for all Analysts)
- CompTIA Network+ Certification
- CompTIA Security+ Certification
- CRISC Certification (recommended for Analysts Tiers 2-3)
- GCIA or GCIH Certification ...

Top 10 Preferred Certifications

Click a certification below to see a list of no-cost training that leads to certification attainment.

1. CompTIA - A+
2. CompTIA - Advanced Security Practitioner (CASP)
3. CompTIA - Network+
4. CompTIA - Security+
5. EC Council - EC-Council Certified Security Analyst (ECSA)
6. EC-Council - EC-Council Certified Ethical Hacker (CEH)
7. GIAC - GIAC Certified Forensic Analyst (GCFA)
8. GIAC - GIAC Certified Forensic Examiner (GCFE)
9. ISC2 - Certified Cyber Forensics Professional (CCFP)
10. ISC2 - Certified Information Systems Security Professional (CISSP)

Professional Development Activities

Click a link below to learn more...

- Apply investigative techniques to incident response
- Coaching
- Conduct a threat assessment
- Cross-training/shadowing/rotations with investigative entities (OSSI, OIG, US-CERT)
- Develop presentation skills (recommended for Analysts Tiers 2-3)
- Job exchange with Research & Forensics, other technical experts (recommended for all Analysts)
- On-the-job coaching/mentoring/rotation/shadowing
- Participate in and/or perform case studies, after-action reports, sandbox activities (recommended for all Analysts)
- Participate in Mentorship program
- Participate in regularly-scheduled sandbox sessions
- Perform security analyses of IT activities
- Prepare a business requirements document...

Junior Cybersecurity Analyst Profile

Description

A Junior Cybersecurity Analyst, sometimes referred to as *Tier 1* support, is Lorem ipsum dolor sit amet, errem saepe referrentur ad usu, et ridens accusamus eum. Ne iusto facilis ceteros vim. Exerci omnium gubergren eam id, eum commodo vidisse saperet ex. Suas mutat elaboraret an nam, an explicari definiebas sed..

Other Possible Titles

- Network Security Analyst/Specialist/Professional
- Attacking, Sensing, and Warning Specialist
- Network Security Analyst
- Detection Analyst
- Signature Creator/Signature Developer (at advanced levels)
- Traffic Analyst
- Event Manager
- Watch Officer

Proficiency Targets

For each of the technical competencies listed below, subject matter experts assigned a proficiency target. Click the Technical Competency to read more about the competency, desired proficiency, and example behaviors and performance standards. (LINK TO LOWER IN THE DOCUMENT)

Technical Competency	(GS-9/11)
Cybersecurity Analysis (Derivative of NICE Specialty Area Computer Network Defense (CND) Analysis)	1
Security Monitoring and Event Analysis*	2
Network Forensics (Derivative of NICE Specialty Area Digital Forensics)	0
Exploitation Analysis	0
Incidence Response	1
Security Engineering – Operations*	1

Key Knowledge, Skills, and Abilities

*This list is relevant only to the Cybersecurity Analyst work role. Other work roles do not contain Key KSA lists.

KSA Description	GS-9/11 Level, Intern - Cybersecurity Analyst, (Service Desk Analyst)
Supervision Level	Directly Supervised
IA and Security Concepts	<ul style="list-style-type: none"> • Knowledge of information assurance (IA) and security concepts (e.g., perimeter defense and confidentiality, integrity, and availability)
Government-approved Standards and Technologies	<ul style="list-style-type: none"> • Knowledge of government-approved standards and technologies; activity tracing to a source (e.g., Internet Protocol (IP) address) to document findings
Security Tools, Capabilities, and Analysis	<ul style="list-style-type: none"> • Knowledge of and ability to use security tools/capabilities • Skill in incident tracking methodologies • Skill in reviewing security tool information to determine appropriate incident escalation points
Querying Logs	<ul style="list-style-type: none"> • Knowledge of querying logs
Threat Identification and Tracking	<ul style="list-style-type: none"> • Skill in threat identification and tracking • Ability to identify potential threats and vulnerabilities by following prescribed protocols
Communication	<ul style="list-style-type: none"> • Ability to communicate in both written and verbal forms, translating technical information into commonly-understood language or terms • Ability to document findings
Event Correlation	<ul style="list-style-type: none"> • Skill in security event information gathering • Skill in performing internal and external research to assist in incident response activities • Ability to maintain situational awareness of security events and incidents...
Network Configuration	<ul style="list-style-type: none"> • Knowledge of collecting and/or reviewing network configuration information • Skill in network analysis through basic...



Ready to Level Up?

To prepare for the GS-12 Cybersecurity Analyst Work Role, [Click here to see Key KSAs, Proficiency Targets, Certifications, and more!](#)

Certifications

At a GS 9 and GS 11 level, subject matter experts recommend you work toward attaining one or more of the following certifications. Click any of the links below to see a list of no-cost training that will help you prepare to take the exam to obtain your certification.

1. [CompTIA – Security+](#)
2. [CompTIA - Advanced Security Practitioner \(CASP\)](#)
3. [CompTIA - Network+](#)
4. [CompTIA - A+](#)
5. [EC Council - EC-Council Certified Security Analyst \(ECSA\)](#)

Technical Competencies for Junior Cybersecurity Analysts

Each Technical Competency is representative of a *Specialty Area* in the NICE Framework*. Some of the HHS competencies have been adjusted to match HHS workforce needs.

Cybersecurity Analysis

The Cybersecurity Analysis (Derivative of NICE Specialty Area Computer Network Defense (CND) Analysis) technical competency requires that staff uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Example Tasks Identified as Part of Competency:

- Prioritizes network traffic for analysis to identify anomalous activity and potential threats to network resources
- Performs incident triage (e.g., coordinates the collection and analysis of intrusion artifacts)
- Investigates, identifies, and analyzes threats that trigger network-based event alerts
- Uses security monitoring tools to capture real-time traffic to determine the presence or activity of running malicious code

[Click Here to see Performance Standards for Cybersecurity Analysis](#)



Click any of the competency titles to see the full competency detail for the Cybersecurity Analyst.

Behavioral Indicators

<p>0 No Foundational Knowledge</p>	<ul style="list-style-type: none"> • Demonstrates no sufficient, applied knowledge, or skills in Cybersecurity Analysis for use in routine work situations. Any awareness, knowledge, or understanding would be considered common or casual, similar to that of a layperson
<p>1 Basic</p>	<ul style="list-style-type: none"> • Under direct guidance, reviews network security tool information and reports all incidents to appropriate escalation points • Follows prescribed, standard operating procedures (SOPs) to handle events identified by security tools in response to new or observed threats • Follows information systems/network security guidelines to support protection and restoration services, and capabilities with supervisor or peer guidance by recognizing and adhering to the components of the Security Plan (e.g., contingency plan, site security plan, risk assessment plan) • Under direct guidance, uses cyber threat analysis tools and technologies to monitor networks to identify anomalous network behavior or traffic patterns against baseline network activity • Under direct guidance, gathers information from various sources to gain situational awareness and assist in event correlation activities • Notifies managers, incident responders, and other security service provider team members of suspected incidents

Criticality

Importance	Required at Entry	Criticality
5 – Extremely Important	2 – Preferred, but Not Required	Extremely Important; Preferred but not Required

Proficiency Targets

Intern (GS-9/11), Cybersecurity Analyst (Service Desk Analyst)

0

Cybersecurity Analyst Performance Standards

Performance **standards*** help all staff develop consistent and measurable standards that can be used when developing annual Performance Management Appraisal Program (PMAP) plans. The examples here are derived from IT and cybersecurity **competencies*** and behavioral indicators and are rooted from the National Institute of Standards and Technology (NIST) National Initiative Cybersecurity Education (NICE) Workforce Framework (NIST SP 800-181).

Recommendations for using this Document

1. Identify up to 3-4 sample performance standards in each competency that are relevant to the position/work role within OCIO and tailor them accordingly. Apply principles of SMART goals: Specific, Measurable, Attainable, Relevant, and Timely.
2. Align the performance standards to appropriate OCIO PMAP *element*. OCIO Standard Elements include:



Competencies

A competency is a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully. Competencies specify the "how" of performing job tasks, or what the person needs to do the job successfully.

Standards

Standards are measures of our behaviors, how we develop and execute a process, and/or what we produce. These measurements (behavioral or product) depend on the type of work we do and can depend on our role, grade, and level of responsibility within our organizations. The performance standards in this dictionary are completely customizable so that, regardless of your level of proficiency, grade, or level of seniority, each person using this dictionary can adapt the standards to create clear, measurable indicators by which to measure performance each year.

Cybersecurity Defense Analysis

Definition

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Work Role(s) Associated with this Competency

1. Cyber Defense Analyst (PR-DA-001) (511)

Performance Standards

Click the desired performance standards you'd like to add to your PMAP

- Gains situational awareness by collecting **XX** network security sensor information to track **XX** network events and activities and report all incidents to **XX** personnel on a monthly/quarterly basis
- Conducts data calls for information from **XX** components for technical solution review by sending out mass correspondence, fielding feedback, and collecting information in an organized and accurate format to achieve **XX**
- Supports **XX** network administrators in the active defense of the enterprise level network controls through protective technologies to achieve **XX**

- Hardens, configures, diagnoses, troubleshoots and/or resolves **XX** hardware, **XX** software, or other **XX** network and system problems using network security knowledge such as **XX**
- Maintains and administers **XX** computer networks and related computing environments to protect, defend, and restore network services and capabilities by doing **XX** on a monthly/quarterly basis
- Participates in the analysis, evaluation, development, coordination, and dissemination of security tools and procedures via **XX** methods to eliminate **XX** system vulnerabilities and threats
- Monitors external data sources such as **XX** to maintain current CND threat condition and determine which security issues may have an impact on the network; assists in the development of signatures and thresholds that trigger network based event alerts and develops draft mitigation recommendations to achieve **XX**

- Analyzes **XX** network alerts from various sources such as **XX** and synthesizes this information to identify new malicious activity within monitored networks and develops network and/or network mitigation strategies to achieve **XX**
- Develops certification documentation and reviews and tracks **XX** number of audit findings to determine risk levels such as **XX** and **XX** and recommends changes to the organization's IA/IS standards and procedures on a monthly/quarterly basis

- Reviews **XX** number of event correlations; validates and approves **XX** number of recommended mitigation efforts based on analysis of network alerts via **XX** methods
- Oversees and coaches **XX** in **XX** network discovery, hardening, configuration, diagnostics, and enterprise-wide mitigation strategies via **XX** methods to achieve **XX** aims
- Ensures system requirements identified in the system security plan are incorporated into the systems development lifecycle process by comparing current authorized systems against established lifecycle processes to achieve **XX** goals

Click to Go Back to
Technical Competencies
List

CLICK TO
COPY ALL
SELECTED

Click to go to the next
competency

CONTACT US

Josh Musicante



joshua.musicante@hhs.gov



[linkedin.com/in/joshua-musicante-3292ba1b/](https://www.linkedin.com/in/joshua-musicante-3292ba1b/)



[@joshuamusicante](https://twitter.com/joshuamusicante)

Sarah Moffat



sarah.moffat@hhs.gov



www.linkedin.com/sarahcmoffat



[@sarahcmoffat](https://twitter.com/sarahcmoffat)

CERTIFICATION ALIGNMENT AND NO-COST TRAINING CATALOG

The screenshot displays an Excel spreadsheet with a green title bar that reads "Certification Alignment and No-Cost Training by NICE Work Role_10172017 - Excel". The ribbon includes tabs for File, Home, Insert, Page Layout, Formulas, Data, Review, View, and ACROBAT. The Home tab is active, showing options for Clipboard, Font, Alignment, Number, Styles, and Cells. The spreadsheet grid shows columns A through M and rows 1 through 21. A red box highlights a blue hyperlink in cell I1 that says "Click here for the Table of Contents". Below this, a text box contains the following instructions:

Instructions: Please review the HHS IT/Cybersecurity Work Roles and Description table in the Table of Contents tab to find the relevant type of work in which you are interested in receiving training. To navigate this Training Guide from the **Table of Contents** tab:

- The **HHS Top 7 Certifications** link at the top of the page will navigate you to the list of certifications most frequently attained at HHS as well as information about no-cost training and other resources associated with the certifications.
- The **Additional Resources** link at the top of the page will navigate you to a list of additional free-training resources to consider.
- The **Integral Certifications Master Sheet** link at the top of the page will navigate you to the Master Certification Sheet which shows the alignment of over 500 identified IT/cybersecurity-related certifications to the HHS IT/Cybersecurity Work Roles.

In the HHS IT/Cybersecurity Work Roles and Description table:

- The **No-Cost Training** links will navigate you to a list of all no-cost training available for this specific Work Role as well as other associated Work Roles.
- The **Integral Certifications** links will list the integral certification for this specific Work Role as well as other associated Work Roles.

At the bottom of the spreadsheet, a red box highlights the sheet navigation bar, which includes tabs for "Instructions", "Table of Contents", "HHS Top 7 Certs", "Addl Resources", and "Integral Certs Master Sheet". The "Instructions" tab is currently selected.

CERTIFICATION ALIGNMENT AND NO-COST TRAINING TABLE OF CONTENTS

Certification Alignment and No-Cost Training by NICE Work Role_10172017 - Excel

Musicante, Joshua (OS/ASA)

HHS Work Role/Certification	Description	No-Cost Training	Integral Certifications
Cyber Defense Analyst (511)	Coordinates Department-wide incident response for (1) threat hunters, 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-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.	Click here for no-cost training for this Work Role	Click here for integral certifications for this Work Role
Cyber Defense Incident Responder (531)	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. Triage, 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.	Click here for no-cost training for this Work Role	Click here for integral certifications for this Work Role
Cyber Instructional Curriculum Developer (711) Cyber Instructor (712)	Focuses on content development, communications, and/or training program management in support of cybersecurity awareness or relevant technical subject domains. Coordinates with all cybersecurity programs at HHS, marketing their programs and capabilities across all modal representatives to support cybersecurity awareness initiatives. May conduct and/or coordinate training of personnel within pertinent 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 cybersecurity exercise projects (e.g. planning and coordinating private sector participation, and developing goals and scenarios).	Click here for no-cost training for this Work Role	Click here for integral certifications for this Work Role

Table of Contents

[Click here for the HHS Top 7 Certifications](#)
[Click here for additional resources](#)
[Click here to view the Integral Certifications Master Sheet](#)

[Instructions](#) | [Table of Contents](#) | [HHS Top 7 Certs](#) | [Addl Resources](#) | [Integral Certs Master Sheet](#) ...

CERTIFICATION ALIGNMENT AND NO-COST TRAINING HHS TOP 7 CERTIFICATIONS

Certification Alignment and No-Cost Training by NICE Work Role_10172017 - Excel

File Home Insert Page Layout Formulas Data Review View ACROBAT Tell me what you want to do... Musicante

Clipboard Font Alignment Number Styles Cells Editing

A1 HHS Top Seven Certifications

HHS Top Seven Certifications

As part of the Federal Cybersecurity Workforce Assessment Act's (FCWAA) December 2016 data collection effort, HHS distributed an employee inventory questionnaire. Employees were asked which certification(s), if any, helped increase quality of work performance. Those top certifications are listed below.

CERTIFICATION	DESCRIPTION	CERTIFICATION AUTHORITY
FAC-PPM (IT CORE)	The Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) is governed by the December 16, 2013 Memo on Revisions to the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) from Office of Federal Procurement Policy (OFPP). As determined by OFPP, all P/PMs assigned to programs or projects must be FAC-P/PM certified at the appropriate level and possess the required experience. The FAC-P/PM certification is required for all P/PMs at the appropriate levels. Additionally, FAC P/PM IT Core-Plus requirements are outlined in OFPP's December 16, 2013 Memo on Revisions to the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM), located on the Federal Acquisition Institute's (FAI) website.	https://www.fai.gov/drupal/certification/program-and-project-managers-fac-ppm
Certified Information Systems Security Professional (CISSP)	Independent information security certification governed by the International Information System Security Certification Consortium, also known as (ISC)². The CISSP curriculum covers subject matter in a variety of Information Security topics. The CISSP examination is based on what (ISC)² terms the Common Body of Knowledge (or CBK). According to (ISC)², "the CISSP CBK is a collection of topics relevant to information security professionals around the world. The CISSP CBK establishes a common framework of information security terms and principles that allow information security professionals worldwide to discuss, debate and resolve matters pertaining to the profession with a common understanding.	https://www.isc2.org
Project Management Professional (PMP)	Project Management Professional (PMP) is an internationally recognized professional designation offered by the Project Management Institute (PMI). PMP is the gold standard of project management certification. Recognized and demanded by organizations worldwide, the PMP validates your competence to perform in the role of a project manager, leading and directing projects and teams.	https://www.pmi.org/certifications
Certified Cloud Security Professional (CCSP)	CCSP is a global credential born from the expertise of the two industry-leading stewards of information systems and cloud computing security, (ISC)² and CSA. The CCSP credential is appropriate and applicable to cloud security in a global	https://www.isc2.org

Instructions Table of Contents **HHS Top 7 Certs** Add Resources Integral Certs Master Sheet ...




CERTIFICATION ALIGNMENT AND NO-COST TRAINING ADDITIONAL RESOURCES

Certification Alignment and No-Cost Training by NICE Work Role_10172017 - Excel

File Home Insert Page Layout Formulas Data Review View ACROBAT Tell me what you want to do...

Clipboard Font Alignment Number Styles Cells

A1 Training Resources only reference free training and/or online independent study courses

Resource	General Program Information	Website
	Skillssoft provides the widest array of integrated learning types to continuously develop and maintain IT skills – including short expert-led videos, video-based eLearning courses, live web-based instructor-led training, free live mentoring services, certification test preparation, and access to tens of thousands of full text online books. Certification support for more than 100 professional IT certification exams from leading software, hardware, networking, web service companies and professional organizations.	https://www.skillssoft.com
	Federal Virtual Training Environment (FedVTE) is an free online, on-demand cybersecurity training system that is available at no charge for government personnel and veterans. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. Several courses also align with a variety of IT certifications. Course proficiency ranges from beginner to advanced levels.	https://fedvte.usalearning.gov
	SANS Cyber Aces is SANS' philanthropic initiative to help individuals discover and develop skills and careers in cybersecurity. SANS donates free, online courses that teach the fundamentals of cybersecurity to program participants, organizes state-wide competitions, and helps connect participants to employers. SANS Cyber Aces Online makes available, free and online, selected courses from the	http://www.cyberaces.org

Instructions Table of Contents HHS Top 7 Certs Addl Resources Integral Certs Master Sheet

CERTIFICATION ALIGNMENT AND NO-COST TRAINING HHS TOP 7 CERTIFICATIONS NO-COST TRAINING

Certification Alignment and No-Cost Training by NICE Work Role_10172017

File Home Insert Page Layout Formulas Data Review View ACROBAT Tell me what you want to do...

Clipboard Font Alignment Number Styles

A1 Click here to return to the Table of Contents

Certified Information Systems Security Professional (CISSP)			
Aligned Skillssoft Training	LMS Asset ID	Course Type	Proficiency
CISSP: Security Principles, Governance, and Guidelines	sp_cisp_a01_it_enus	Skillssoft Course	Advanced
CISSP: Risk Management	sp_cisp_a02_it_enus	Skillssoft Course	Advanced
CISSP: Asset Security	sp_cisp_a03_it_enus	Skillssoft Course	Advanced
CISSP: Security Engineering Part 1	sp_cisp_a04_it_enus	Skillssoft Course	Advanced
CISSP: Security Engineering Part 2	sp_cisp_a05_it_enus	Skillssoft Course	Advanced
CISSP: Communication & Network Security Design	sp_cisp_a06_it_enus	Skillssoft Course	Advanced
CISSP: Identity and Access Management	sp_cisp_a07_it_enus	Skillssoft Course	Advanced
CISSP: Security Assessment and Testing	sp_cisp_a08_it_enus	Skillssoft Course	Advanced
CISSP: Security Operations Part 1	sp_cisp_a09_it_enus	Skillssoft Course	Advanced
CISSP: Security Operations Part 2	sp_cisp_a10_it_enus	Skillssoft Course	Advanced
CISSP: Security Operations Part 3	sp_cisp_a11_it_enus	Skillssoft Course	Advanced
CISSP: Software Development Security	sp_cisp_a12_it_enus	Skillssoft Course	Advanced
Supplemental Training	LMS Asset ID	Course Type	Proficiency
TestPrep Systems Security Certified Practitioner (SSCP)	sp_sscp_a01_tp_enus	Skillssoft Testprep Exams	Intermediate
TestPrep Certified Information Systems Security Professional (CISSP)	sp_cssp_a01_tp_enus	Skillssoft Testprep Exams	Advanced
Mentoring Systems Security Certified Practitioner (SSCP)	mntsscp2ed	Skillssoft Mentoring Asset	Intermediate
Mentoring Certified Information Systems Security Professional (CISSP)	mntcissp	Skillssoft Mentoring Asset	Advanced
CISSP: Network Security and Vulnerability Management	79290	Skillssoft Video	
CISSP: Securing Networks and Hardware	79279	Skillssoft Video	
Cloud Computing Technology Fundamentals: Cloud Network Infrastructure Security	89951	Skillssoft Video	
Aligned FedVTE Training	Course Length/Type	Proficiency	
(ISC)2 CISSP: ISSMP Certification Prep	14 hours/Exam Prep	Advanced	

HHS Top 7 Certs Addl Resources Integral Certs Master Sheet FAC-PPM CISSP PMP CC ...

CERTIFICATION ALIGNMENT AND NO-COST TRAINING WORK ROLE NO-COST TRAINING

Certification Alignment and No-Cost Training by NICE Work Role_10172017 - Excel

File Home Insert Page Layout Formulas Data Review View ACROBAT Tell me what you want to do... Musicante, Joshua

Clipboard Font Alignment Number Styles Cells Editing

A1 Click here to return to the Table of Contents

	A	B	C	D
1	Click here to return to the Table of Contents		Click here to view the integral certifications for this Work Role	
2			Click here to view the Integral Certifications Master Sheet	
3	Cyber Defense Analyst (511)			
4	Other Associated Work Role(s): Cyber Defense Forensics Analyst (212), Law Enforcement/CounterIntelligence Forensics Analyst (211), Exploitation Analyst (121)			
5	CompTIA Security+			
6	Certified Information Systems Security Professional (CISSP)			
7	Global Information Assurance Certification (GIAC)			
8	Syracuse University Veterans Career Transition Program (VCTP) via SANS Cyber Talent Immersion Academy		Type	Proficiency
9	GIAC Security Essentials Certification (GSEC)		Refer to SANS Immersion at https://www.sans.org	Intermediate
10	GIAC Certified Incident Handler (GCIH)		Refer to SANS Immersion at https://www.sans.org	Intermediate
11	GIAC Certified Intrusion Analysis (GCIA)		Refer to SANS Immersion at https://www.sans.org	Intermediate
12	GIAC Certified Forensic Examiner (GCFE)		Refer to SANS Immersion at https://www.sans.org	Intermediate
13	GIAC Certified Web Application Penetration Tester (GWAPT)		Refer to SANS Immersion at https://www.sans.org	Intermediate
14	GIAC Certified Enterprise Defender (GCED)		Refer to SANS Immersion at https://www.sans.org	Intermediate
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				

Auth Offcl & Dsgntng Rep Trng COMSEC Manager Trng **Cyber Defense Analyst Trng** Cybr Dfr ...

CERTIFICATION ALIGNMENT AND NO-COST TRAINING WORK ROLE CERTIFICATION

ALIGNMENT MASTER SHEET

Certification Alignment and No-Cost Training by NICE Work Role_10172017 - Excel

File Home Insert Page Layout Formulas Data Review View ACROBAT Tell me what you want to do... Musicante, Joshua (OS/ASA) Share

Clipboard Font Alignment Number Styles Cells Editing WebEx

X546 Yes

Integral Certifications by NICE Work Role			500 - Protect and Defend									
Click here to return to the Table of Contents			Network Services	Systems Administration	Systems Analysis	Cybersecurity Defense Analysis	Cybersecurity Defense Infrastructure Support	Incident Response	Vulnerability Assessment and Management	Risk Management		Software Dev
Vendor	Certifications	Website	Network Operations Specialist (441)	System Administrator (451)	Systems Security Analyst (461)	Cyber Defense Analyst (511)	Cyber Defense Infrastructure Support Specialist (521)	Cyber Defense Incident Responder (531)	Vulnerability Assessment Analyst (541)	Authorizing/Designating Representative (611)	Security Control Assessor (612)	Software Developer (621)
ISC2	Certified Cloud Security Professional (CCSP)	https://www.isc2.org/ccsp/default.aspx		Yes	Yes		Yes		Yes	Yes	Yes	
ISC2	Certified Cyber Forensics Professional (CCFP)	https://www.isc2.org/ccfp/default.aspx				Yes	Yes	Yes				
ISC2	Certified Information Systems Security Professional (CISSP)	https://www.isc2.org/cissp/default.aspx	Yes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISC2	Certified Secure Software Lifecycle Professional (CSSLP)	https://www.isc2.org/csslp/default.aspx			Yes							Yes
ISC2	CISSP Information Systems Security Architecture Professional (CISSP-ISSAP)	https://www.isc2.org/issap.aspx										
ISC2	CISSP Information Systems Security Engineering Professional (CISSP-ISSEP)	https://www.isc2.org/issep.aspx	Yes		Yes		Yes					

Integral Certs Master Sheet | PAC-PPM | CISSP | PMP | CCSP | CISM | CCNA | CISSP - ISSMP