



CYBERSPACE WORKFORCE

Cyber Excepted Service

March 2, 2016



Agenda



- **Challenges with Determining Who Is the Cyber Workforce**
 - Defining the Cyber Workforce
 - Occupational Series vs Work Roles
 - Initial Efforts to Identify the Cyber Workforce
 - New Congressional Mandate to Code the Cyber Workforce
- **Challenges with New Excepted Service Authority**
 - Defining the Scope
 - Determining What and How Much We Can Leverage
 - Establishing Rates of Pay



Notional Representation of the Cyber Workforce



Cyber Workforce

Size not to scale

Cyber IT
Workforce

Cybersecurity
Workforce

Cyber
Effects
Workforce

Intelligence
Workforce
(Cyber)

*Intelligence
Workforce*

*Cyber
Mission
Force*

Cyber Workforce Skill Categories Definitions



Cyberspace IT Workforce: Personnel, who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.

Cybersecurity Workforce: Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.

Cyberspace Effects Workforce: Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

Intelligence Workforce (Cyberspace): Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.

Source: DoDD 8140.01 – August 11, 2015

IT/Cyber Occupational Series and Relationships

CORE > 500 employees in the Series	2210 IT Management (MCO)		1550 Computer Science (MCO)		0391 Telecommunications (MCO)		0335 Computer Clerk and Assistant		 Within the IT Functional Community		
CORE <500 employees in the Series	0306 Government Information		0332 Computer Operation		0390 Telecommunications Processing		0392 General Telecommunications			0394 Communications Clerical	
	1410 Librarian		1411 Library Technician		1412 Technical Information Services		1420 Archivist			1421 Archives Technician	
	1499 Library & Archives Student Trainee		2299 IT Management Student Trainee		2502 Telecommunications Mechanic		2504 Wire Comms/ Cable Splicing				
Tier 1 - Strong Relationship/ Many cyber	0850 Electrical Engineering		0854 Computer Engineering		0855 Electronics Engineering		0856 Electronics Technical			1515 Operations Research	
Tier 2 - Some cyber	0080 Security	0501 Financial Administration & Program		0511 Auditing	0801 General Engineering		1701 General Education & Training		1801 General Inspection, Investigation, Enforcement, and Compliance		
									1805 Investigative Analysis	1811 Criminal Investigation	
COMMON - Could be working	0301 Misc Admin & Program		0340 Program Management		0343 Management & Program Analysis		1101 General Business and Industry		<i>And others still to be determined</i>		

Cyber Work Roles – 53 to Date



- Software Developer
- Systems Developer
- Requirements Planner
- Enterprise Architect
- R&D Specialist
- T&E Specialist
- Database Administrator
- Data Analyst
- Knowledge Manager
- Tech Support Specialist
- Network Ops Specialist
- Cyber Instructor
- Instructor/Curriculum Developer
- Cyber WF Development & Mgmt
- IT Invest/Portfolio Manager
- IT Project Manager
- Program Manager
- Product Support Manager
- IT Program Audit
- Authorizing Official
- Security Control Assessor
- Information Systems Security Mgr
- Secure Software Assessor
- Security Architect
- Info Systems Security Developer
- Systems Security Analyst
- COMSEC Manager

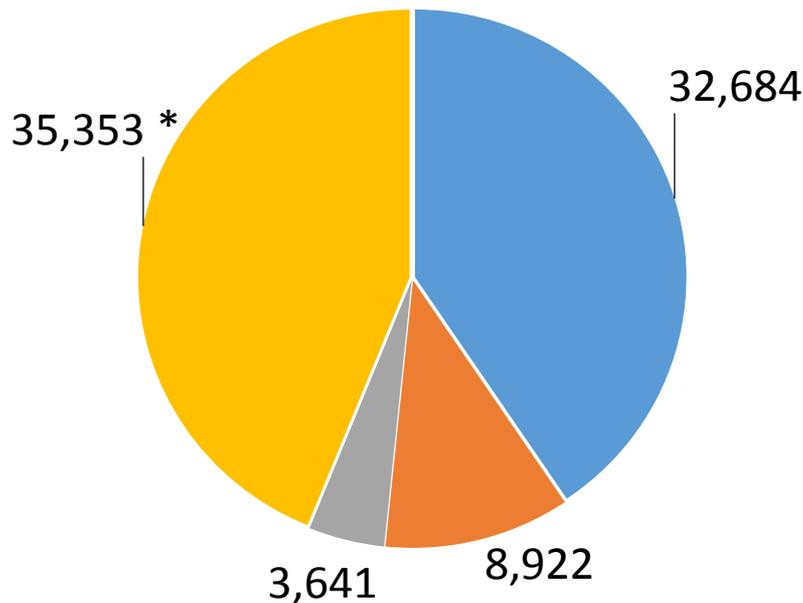
- Have not been coded yet in existing systems
- May align to multiple series
- May select up to 3 per position
- OPM pilot project to code to higher order specialty areas had some issues
 - More time & communication needed for rollout
 - ~200 series identified
- DISA pilot showed 4-5 series per specialty area
- New Congressional mandate for FY2016-2018.

- Cyber Defense Analyst
- Cyber Defense Infrastructure Support Specialist
- Cyber Def. Incident Responder
- Vulnerability Analyst
- Warning Analyst
- Exploitation Analyst
- Cyber Policy/Strat Planner
- Cyber Crime Investigator
- Forensics Analyst
- Cyber Def Forensics Analyst
- System Administrator
- Executive Cyber Leadership
- Legal Advisor
- Mission Assessment Specialist
- Target Digital Network Analyst
- Target Analyst Reporter
- Target Developer
- Interactive Operator
- Cyber Operations Planner
- Integration Planner
- All Source Analyst
- All Source Collection Manager
- All Source Collection Reqmts Mgr
- Cyber Intelligence Planner
- Multi Discipline Language Analyst

Initial Federal Cyber Coding Effort



2210 Series



- DoD Coded
- Other Federal Coded
- DoD Not Coded
- Other Federal Potentially Not Coded

- Guidance was to code to the NICE Cybersecurity Workforce Framework 1.0
- Focused largely on the IT Management 2210 series - the largest cyber series
- 90% of all cyber coded positions (41.6K) were in the 2210 series
- Approximately 44% (~35K) of all 2210 series positions were not coded
- DoD did meet the OPM mandate to code 90% of the 2210 series by Sept 30, 2014

*estimate, based on number of federal 2210 personnel in Fedscope

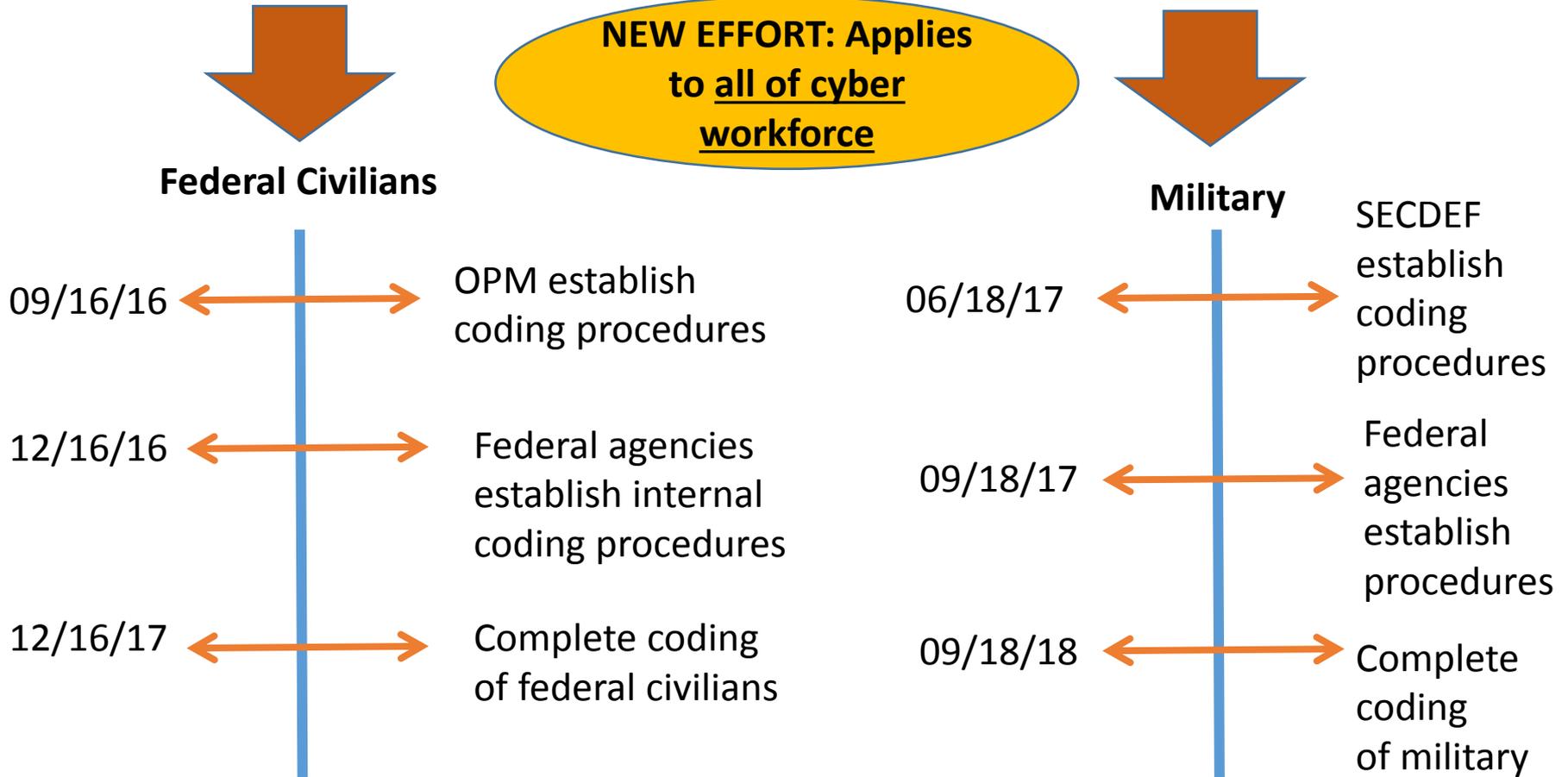
Federal Cybersecurity Workforce Assessment Act of 2015



Contained in the Consolidated Appropriations Act of 2016

JUNE 2016

New Federal Work Role Coding Structure to Be Established



New DoD Excepted Service Provision Scope



- **FY2016 National Defense Authorization Act (NDAA) Section 1107**
 - Amends Chapter 81 to add new Section 1599F – “United States Cyber Command Recruitment and Retention”
 - Authorizes the Secretary of Defense to establish qualified positions in the Title 10 Excepted Service determined necessary to carry out the responsibilities of the USCYBERCOM, including:
 - Positions held by staff of the headquarters of USCYBERCOM
 - Positions held by elements of the USCYBERCOM enterprise relating to cyberspace operations, including elements assigned to the Joint Task Force DoD Information Networks (JTF-DoDIN) [Defense Information Systems Agency]
 - Positions held by elements of the Military Departments supporting USCYBERCOM

DoD Implementation Plan



- The Title 10 Excepted Service Authority becomes effective 30 days after the date that SECDEF provides a plan for implementation to the congressional committees. Implementation Plan must include:
 - Assessment of the current scope of the positions covered by the authority.
 - A plan for use of the authority.
 - An assessment of the anticipated workforce needs of USCYBERCOM across the future-years defense plan.

Notional Governance Structure



- DoD Cyber Workforce Management Board
 - Authorized by DoDD 8140.01 of August 11, 2015, “Cyberspace Workforce Management”
 - Tri-chair: OUSD(Policy) OR Principal Cyber Advisor; OUSD(Personnel & Readiness); DoD CIO
 - DoD CIO will serve as Secretariat
 - Charter being developed – approx 60 days to signature
- Excepted Service Working Group under the Board
 - Initial Membership: DoD CIO, OUSD(I), Principal Cyber Advisor, OUSD(P), OUSD(P&R), CYBERCOM, DCPAS
 - Working Group will commence work while Board Charter is being approved
 - Will continue to build out membership, joint structure for management

DoD Initial Strategy



- Preliminary work to date
 - Excepted Service Workshop - December 2015
 - Seniors Meeting - February 2016
 - First Working Group Meeting - February 2016
- DoD opening position
 - Partner with other communities/organizations – OUSD(I) and DHS
 - Leverage existing policy where possible
 - Emulate NSA where applicable
 - Use existing technology – DCIPS or DCPDS
 - Get lessons learned from previous implementation of Excepted Service
 - Determine phased roll out
 - Minimize cost

DoD vs DHS Authorities



	DoD	DHS
AUTHORITY	FY2016 National Defense Authorization Act (Dec 2015)	Border Patrol Agent Pay Reform Act of 2014 (PL 113-277) (Dec 2014)
SCOPE	Cyber Operations, Support to CYBERCOM	Cybersecurity
APPLICATION	USCYBERCOM, MILDEPS, DISA and potentially others	US Secret Service, FEMA, ICE, CBP, USCIS, FLETC, TSA, US Coast Guard
SENIOR SERVICE APPLICABILITY	TBD	YES
COMPENSATION SETTING	YES	YES
COLLECTIVE BARGAINING	YES	YES
RIGHT TO REFUSE CONVERSION	YES	YES
IMPLEMENTATION PLAN	Required by Congress prior to implementation	Required by Congress 120 days after signature of Act

Compensation Issues



- Limited pay data in for some cyber roles - not yet found in mainstream compensation studies
- Pay grades or pay bands
 - Which type of pay system best supports the broad scope of cyber
 - Should they apply to all cyber roles or just some
 - Should there be one pay system applied to all organizations
- Some entities with cyber personnel already have separate pay systems
- Technical expertise to develop and implement new pay system

Way Ahead



- Implement the DoD Cyber Workforce Framework and work roles
 - Identify the cyber workforce
 - Develop classification and performance measurements – what do high performing cyber personnel look like
- Develop an Excepted Service plan that covers from short term to 5 years from now – where does the Department want to be
- Focus on 3-part solution: Policy, Technology, Operations
- Submit Implementation Plan to Congress