SUBJECT: Identifying, Addressing, and Reporting Cybersecurity Work Roles of Critical Need

EFFECTIVE DATE: Upon release of this HR Bulletin

EXPIRATION DATE: Effective until superseded or revoked


REVISIONS: The Department of Commerce must determine cybersecurity Work Roles of Critical Need as part of the Federal Cybersecurity Workforce Assessment Act of 2015 (Act).

PURPOSE: This bulletin provides the implementation plan for the Department of Commerce (Department) to follow guidance established by the Office of Personnel Management (OPM), which upholds the requirements of the Act. OPM has requested that Federal agencies identify and report information technology (IT), cybersecurity, and other cyber-related Work Roles of Critical Need. The preliminary report to OPM is due on August 31, 2018, and an additional report is due by April 30, 2018; subsequent reports will be required annually through 2022.

BACKGROUND: Beginning in 2013, under the Special Cybersecurity Workforce Project, Federal agencies were tasked to identify and code positions that perform cybersecurity work within the IT Management Series (2210 series). Agencies were later tasked with identifying and coding all positions with appropriate cybersecurity codes. The initial coding aligned with an early version of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The intention was to provide standardization across the public, private, and academic sectors to define cybersecurity work, as well as the common set of tasks and the knowledge, skills, and abilities required to perform cybersecurity work. The Department met the objectives of the initial Special Cybersecurity Workforce Project.

The Act required OPM to establish procedures to implement the next NICE coding structure. The new structure was updated to include work roles and associated codes, and was broadened to include not only cybersecurity functions, but also IT and cyber-related functions. The updated codes incorporated a three-digit code, in place of the former two-digit codes, and allowed for up to
three codes to be assigned per position. The Department met the requirements of the Act and OPM guidance to ensure that all positions were reviewed and coded by April 4, 2018.

Since all positions have been identified and coded, the Act requires the Department to identify and report IT, cybersecurity, and other cyber-related Work Roles of Critical Need.

**COVERAGE:** Applies to all Servicing Human Resources Offices (SHROs) in the Department.

**POLICY:** In order to complete the requirements of the Act, as defined in OPM’s “Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need,” the Department must identify IT, cybersecurity, and other cyber-related Work Roles of Critical Need in the workforce; and submit a report to OPM describing the roles identified, and substantiating the critical-need designation.

**Process**

**SHROs:** The SHROs, in conjunction with their Chief Information Officer (CIO) community counterparts, are required to work with managers/supervisors in their serviced areas to identify Work Roles of Critical Need, to determine root causes, and to develop an action plan with metrics and targets to address and mitigate root causes and shortages. Each SHRO and CIO bureau office must have a designated point of contact to co-manage the initiative.

**Identifying Work Roles of Critical Need**

Work Roles of Critical Need are work roles deemed as having the greatest skill shortages, in terms of staffing levels and/or proficiency/competency levels, current and emerging shortages, and mission criticality or importance. Each bureau must use its “Work Roles” spreadsheet (to be provided to the bureau) to identify all Work Roles of Critical Need. All work roles coded as of May 1, 2018, are included on each spreadsheet as a reference. Additionally, bureaus may utilize an optional Cyber Staffing Resource Chart (to be provided by the bureau), in order to assist in workforce planning. It is important to keep in mind that all work roles are recorded, rather than recording individual positions. For example, if an employee has two three-digit codes, then they will have two codes recorded on both the “Work Roles” spreadsheet and the optional Cyber Staffing Resource Chart.

**Determine Root Causes of Shortages in Work Roles of Critical Need**

Each bureau must use its “Work Roles” spreadsheet to identify the root cause. Root causes may involve a range of issues such as talent pipeline, recruitment/outreach, hiring, retention, development/training, performance management, and resources/budget. All other causes should be identified and described as well.

**Develop Action Plan with Metrics and Targets to Address and Mitigate Root Causes and Shortages in Work Roles of Critical Need**

Once bureaus have identified the root cause for shortages, they must complete OPM’s template for each Work Role of Critical Need. Completing these templates will include developing an action
plan to address and mitigate the root causes identified, and establishing metrics and targets for gauging success in mitigating the root causes and shortages.

**Government-wide Time Line**

- August 31, 2018 – All agencies must identify IT, cybersecurity, and other cyber-related Work Roles of Critical Need, and root causes, to OPM in a preliminary report.
- April 30, 2019 – All agencies must provide a complete report to OPM. This report includes developing action plans with metrics and targets to address and mitigate root causes and shortages in Work Roles of Critical Need.
- April 2020 – Annual report due to OPM.
- April 2021 – Annual report due to OPM.
- April 2022 – Annual report due to OPM.

**Department Timeline**

- July 13, 2018 – SHROs and CIO counterparts review bulletin and discuss responsibilities.
- July 20, 2018 – SHROs meet with all managers/supervisors to discuss new requirements.
- August 17, 2018 – SHROs provide completed “Work Roles” spreadsheets to program manager in order to complete preliminary reporting requirements to OPM.
- March 1, 2019 – SHROs provide completed corresponding templates for each Work Role of Critical Need.
- March 1, 2020 – SHROs provide complete report.
- March 1, 2021 – SHROs provide complete report.
- March 1, 2022 – SHROs provide complete report.

**Reporting Requirements**

The SHROs must provide completed spreadsheet and templates by the designated date above to the Program Manager.


**OFFICE OF POLICY AND PROGRAMS:** Valerie Smith, Director, VSmitth@doc.gov, (202) 482-0272

**PROGRAM MANAGER:** Mary O’Connor, MOConnor@doc.gov, (202) 482-2080
## AGENCY LIST OF CYBERSECURITY WORK ROLES OF CRITICAL NEED

### Agency: SAMPLE - Commerce

#### Agency POC:

**INSTRUCTIONS:** In column C, mark all Work Roles this agency has determined as the Work Roles of Critical Need (WRCN) and then complete the next three sections (columns D - O) for only those WRCNs.

This report is due to OHRM no later than August 17, 2018 (send to MOConnor@doc.gov)

### Work Roles of Critical Need (WRCN)

<table>
<thead>
<tr>
<th>WRCN Title</th>
<th>OPM Code</th>
<th>Work Roles Coded as WRCN</th>
<th>Mark All That Apply</th>
<th>Stuffing Levels</th>
<th>Proficiency/Competency Levels</th>
<th>Current</th>
<th>Emerging</th>
<th>Talent Pipeline</th>
<th>Retention</th>
<th>Hiring</th>
<th>Development/Mgt</th>
<th>Performance</th>
<th>Resources/Budget</th>
<th>Other (describe)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Securely Provision Category

- Cyber Security Officer/Manager and Representative 611
- Security Control Officer 612
- Software Developer 621
- Security Software Assurance 622
- Cryptographic Manager 651
- Security Analyst 652
- Research & Development Specializi 661
- Systems Requirements Planner 662
- System Testing and Evaluation Specialist 671
- Information Systems Security Developer 672
- Systems Developer 673

### Operate and Maintain Category

- Database Administrator 421
- Data Analyst 422
- Knowledge Manager 431
- Technical Support Specialist 441
- Network Operations Specializi 442
- System Administrator 451
- Systems Security Analyst 461

### Operate and Govern Category

- Cyber Legal Advisor 711
- Cyber Institutional Curriculum Developer 712
- Cyber Intelligence 721
- Information Systems Security Manager 722
- Communications Security (COMSEC) Manager 731
- Cyber Workforce Developer and Manager 732
- Cyber Policy and Strategy Planner 733
- Cyber Defense Infra Law 734
- Program Manager 751
- IT Project Manager 752
- Product Support Manager 753
- IT Security/Officer Manager 754
- IT Program Auditor 755

### Protect and Defend Category

- Cyber Defense Analyst 511
- Cyber Defense Information Support Specializi 512
- Cyber Defense Incident Respond 513
- Cyber Defense Assessment Analyst 514

### Analyze Category

- Warning Analyst 111
- Exploitation Analyst 112
- All Source Analyst 113
- Threat Intelligence Specializi 114
- Target Network Analyst 115
- Multi-Agency HUMINT Analyst 116

### Collect and Operate Category

- All Source Collection Manager 311
- All Source Collection Requirements Manager 312
- Cyber Intelligence 313
- Cyber Ops Planner 314
- Portal Integration Planner 315
- Cyber Operator 316

### Investigate Category

- Cyber Investigator 211
- Forensics Analyst 212
- Cyber Defense Forensics Analyst 213

### Complain and Complain

- Cyber Crime Investigator 221
- Forensic Analyst 222
- Cyber Defense Incident Responder 223
- Vulnerability Assessment Analyst 224

### Mission Assessment Specializi

- Mission Assessment Specialist 111
- Target Developer 112
- Target Network Analyst 113
- Multi-Disciplined Language Analyst 114

### Collect and Operate

- All Source-Collection Manager 311
- All Source-Collection Requirements Manager 312
- Cyber Intelligence 313
- Cyber Ops Planner 314
- Portal Integration Planner 315
- Cyber Operator 316

### Analyze

- Warning Analyst 111
- Exploitation Analyst 112
- All-Source Analyst 113
- Threat Intelligence Specializi 114
- Target Network Analyst 115
- Multi-Agency HUMINT Analyst 116

### Collect and Operate

- All Source-Collection Manager 311
- All Source-Collection Requirements Manager 312
- Cyber Intelligence 313
- Cyber Ops Planner 314
- Portal Integration Planner 315
- Cyber Operator 316

### Investigate

- Cyber Investigator 211
- Forensics Analyst 212
- Cyber Defense Forensics Analyst 213

### Mission Assessment Specializi

- Mission Assessment Specialist 111
- Target Developer 112
- Target Network Analyst 113
- Multi-Disciplined Language Analyst 114

### Collect and Operate

- All Source-Collection Manager 311
- All Source-Collection Requirements Manager 312
- Cyber Intelligence 313
- Cyber Ops Planner 314
- Portal Integration Planner 315
- Cyber Operator 316

### Analyze

- Warning Analyst 111
- Exploitation Analyst 112
- All-Source Analyst 113
- Threat Intelligence Specializi 114
- Target Network Analyst 115
- Multi-Agency HUMINT Analyst 116

### Collect and Operate

- All Source-Collection Manager 311
- All Source-Collection Requirements Manager 312
- Cyber Intelligence 313
- Cyber Ops Planner 314
- Portal Integration Planner 315
- Cyber Operator 316

### Investigate

- Cyber Investigator 211
- Forensics Analyst 212
- Cyber Defense Forensics Analyst 213
## Cyber Staffing Resource Chart

**Agency Name:** Department of Commerce

**Cyber Code - Cyber Work Role**

<table>
<thead>
<tr>
<th>Cyber Code</th>
<th>Cyber Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>111</td>
<td>All-Source Analyst</td>
</tr>
<tr>
<td>112</td>
<td>All-Source Assessment Specialist</td>
</tr>
<tr>
<td>122</td>
<td>Explanatory Analyst</td>
</tr>
<tr>
<td>131</td>
<td>Legal Developer</td>
</tr>
<tr>
<td>151</td>
<td>Target Network Analyst</td>
</tr>
<tr>
<td>141</td>
<td>Planning Analyst</td>
</tr>
<tr>
<td>191</td>
<td>All-Source Language Analysis/Targeting Analyst</td>
</tr>
<tr>
<td>211</td>
<td>Planning Analyst</td>
</tr>
<tr>
<td>221</td>
<td>Cyber Crime Investigator</td>
</tr>
<tr>
<td>311</td>
<td>All-Source Collection Manager</td>
</tr>
<tr>
<td>322</td>
<td>Cyber Co-Deputy</td>
</tr>
<tr>
<td>331</td>
<td>Cyber Intel Planner</td>
</tr>
<tr>
<td>332</td>
<td>Cyber Ops Planner</td>
</tr>
<tr>
<td>211</td>
<td>Cyber Defense Analyst</td>
</tr>
<tr>
<td>333</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>351</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>411</td>
<td>Technical Support Specialist</td>
</tr>
<tr>
<td>421</td>
<td>Database Administrator</td>
</tr>
<tr>
<td>422</td>
<td>Cyber Analyst</td>
</tr>
<tr>
<td>431</td>
<td>Knowledge Manager</td>
</tr>
<tr>
<td>441</td>
<td>Research Operations Specialist</td>
</tr>
<tr>
<td>451</td>
<td>Systems Administrator</td>
</tr>
<tr>
<td>461</td>
<td>Cyber Security Analyst</td>
</tr>
<tr>
<td>452</td>
<td>Cyber Security Analyst</td>
</tr>
<tr>
<td>511</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>512</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>531</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>541</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>561</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>611</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>621</td>
<td>Software Developer</td>
</tr>
<tr>
<td>631</td>
<td>Software Developer</td>
</tr>
<tr>
<td>641</td>
<td>Systems Requirements Planner</td>
</tr>
<tr>
<td>661</td>
<td>Research/Development/Security/Assessment/Support</td>
</tr>
<tr>
<td>671</td>
<td>Systems Testing and Evaluation Specialist</td>
</tr>
<tr>
<td>681</td>
<td>Systems Development/Security/Assessment/Support</td>
</tr>
<tr>
<td>711</td>
<td>Cyber Command/Control/Security/Assessment/Support</td>
</tr>
<tr>
<td>721</td>
<td>Cyber Instructor</td>
</tr>
<tr>
<td>731</td>
<td>Cyber Legal Advisor</td>
</tr>
<tr>
<td>741</td>
<td>Cyber Compliance Manager</td>
</tr>
<tr>
<td>751</td>
<td>Cyber Workforce Developer and Manager</td>
</tr>
<tr>
<td>761</td>
<td>Cyber Policy and Programs</td>
</tr>
<tr>
<td>771</td>
<td>Cyber Program Manager</td>
</tr>
<tr>
<td>781</td>
<td>Cyber Project Manager</td>
</tr>
<tr>
<td>811</td>
<td>Product Support Manager</td>
</tr>
<tr>
<td>821</td>
<td>IT Development/Support Manager</td>
</tr>
<tr>
<td>831</td>
<td>IT Program Auditor</td>
</tr>
<tr>
<td>841</td>
<td>Executive/Cyber Leadership</td>
</tr>
</tbody>
</table>

**STARTING POINT [DATA FROM BEGINNING OF MEASUREMENT YEAR]**

| (A) BASLINE - Number of Work Roles On Board as of 9/30/2018 | (B) Target for Number of Work Roles to Reach by End of FY2019 (Sept 30, 2019) | (C) Projected Attrition for FY2019 and FY 2020 (Oct 1, 2019 - Sept 30, 2020)(Enter Negative Numbers for Attrition) | (D) Target for Number of Work Roles to Reach by End of FY2020 (Sept 30, 2020) | (E) Projected Attrition for FY2020 (Oct 1, 2020 - Sept 30, 2020)(Enter Negative Numbers for Attrition) | (F) Target for Number of Work Roles to Reach by End of FY2022 (Sept 30, 2022) | (G) Projected Attrition for FY2021 and FY 2022 (Oct 1, 2021 - Sept 30, 2022)(Enter Negative Numbers for Attrition) | (H) Staffing Gap (J) Surplus (+) to Close FY2019 (Including Attrition) (A) + (C) - (B) | (I) Staffing Gap (J) Surplus (+) to Close FY2020 (Including Attrition) (A) + (C) + (E) - (D) | (J) Staffing Gap (J) Surplus (+) to Close FY2022 (Including Attrition) (A) + (C) + (E) + (G) - (F) |
|-------------------------------------------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|

<table>
<thead>
<tr>
<th>STARTING POINT [DATA FROM BEGINNING OF MEASUREMENT YEAR]</th>
<th>(A) BASLINE - Number of Work Roles On Board as of 9/30/2018</th>
<th>(B) Target for Number of Work Roles to Reach by End of FY2019 (Sept 30, 2019)</th>
<th>(C) Projected Attrition for FY2019 and FY 2020 (Oct 1, 2019 - Sept 30, 2020)(Enter Negative Numbers for Attrition)</th>
<th>(D) Target for Number of Work Roles to Reach by End of FY2020 (Sept 30, 2020)</th>
<th>(E) Projected Attrition for FY2020 (Oct 1, 2020 - Sept 30, 2020)(Enter Negative Numbers for Attrition)</th>
<th>(F) Target for Number of Work Roles to Reach by End of FY2022 (Sept 30, 2022)</th>
<th>(G) Projected Attrition for FY2021 and FY 2022 (Oct 1, 2021 - Sept 30, 2022)(Enter Negative Numbers for Attrition)</th>
<th>(H) Staffing Gap (J) Surplus (+) to Close FY2019 (Including Attrition) (A) + (C) - (B)</th>
<th>(I) Staffing Gap (J) Surplus (+) to Close FY2020 (Including Attrition) (A) + (C) + (E) - (D)</th>
<th>(J) Staffing Gap (J) Surplus (+) to Close FY2022 (Including Attrition) (A) + (C) + (E) + (G) - (F)</th>
</tr>
</thead>
</table>

### Legend

- **Numbers in cells in blue** must be completed by the agency at the end of the measurement year.
- **Yellow cells show values that will be entered or calculated by the computer program**.
- **Enter information about dates and names in the rows at the top of the table**.
- **Underlined dates in the table** will be entered by the computer program based on what the agency enters at the top of the table.
- **Enter names of MCOs on the table’s rows**. Gaps, additions, and losses should be shown as negative numbers and surpluses as positive numbers.

**Enter information about dates and names in the rows at the top of the table. Underlined dates in the table will be entered by the computer program based on what the agency enters at the top of the table.**