



Department of the Navy

# CYBER SECURITY WORKFORCE

## SCHEDULE A HIRING AUTHORITY FINAL IMPLEMENTING GUIDANCE



Prepared by:  
DONCIO  
USMC  
SPAWAR  
NAVY CYBER FORCES  
FFC  
OCHR  
HRO  
HRSC



# Table of Contents

I. Introduction

II. Coverage

III. Authority

IV. Position Description Statement Required

V. Qualifications Required

VI. Selective Placement Factors

- Option Factor - Certifications
- 391
- 854
- 855
- 1515
- 1550
- 2210

VII. Hiring Methodology

VIII. Positions in Alternative Personnel Systems

IX. DCPDS Coding

X. Allocations

XI. Reporting

Appendix A: References



## I. Introduction

The Department of Defense requested and received the authority to staff certain cyber security positions worldwide. This authority is limited to positions that require unique qualifications not currently established by the Office of Personnel Management to perform such functions as cyber risk and strategic analysis incident handling and malware/vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber related infrastructure inter-dependency analysis. Specific references associated with this authority are indicated in Part IX of this guidance. In order to use this authority, Department of the Navy was required to create selective placement factors to be used as part of the qualifications for these positions.

Human resources and information technology professionals collaborated across the Department to address the mission-critical need in Cyber Security. The Office of Civilian Human Resources partnered with Fleet Forces, Marine Corps, SPAWAR, NETWARCOM, Human Resource Service Centers, Human Resource Offices and the DON CIO to deploy this new Schedule A Hiring Authority. The DON has been authorized to fill 1013 positions. The effort is in direct support of the emergent needs identified with the newly created Department of the Navy Cyber Forces Command. This guidance will be updated and reissued as needed.

## II. Coverage

This authority covers positions GS-9 through 15 (or equivalent) in the following occupations: 0391; 0854; 0855; 1515; 1550; 2210 requiring cyber security skills and knowledge as described above. This authority is limited to 1013 positions across the Department of the Navy. No new appointments may be made under this authority after December 31, 2012 or the date on which the Office of Personnel Management establishes applicable qualification standards whichever is earlier.

## III. Authority

DoD Schedule A Authority 213.3106(b) (11) must be used for hiring under his authority.

## IV. Position Description Statement Required

This is an Excepted Service Cyber Security Workforce Schedule A Hiring Authority position subject to the laws, regulations and requirements outlined in 5 CFR part 302; the Office of Personnel and Management (OPM) letter of 10 November 2009 and 3 May 2010, the Department of Defense (DoD) Memorandum of 25 March 2010, and the



Department of the Navy Implementing Guidance of 30 Jul 2010. This position requires unique qualifications not currently established by OPM.

## V. Qualification Requirements

One year of directly related experience as described in the duties statement of the position description. Additionally candidates are required to meet the selective placement factor appropriate to the occupation and grade level of the position to be filled as described in this guidance. Only the Selective Placement Factors described herein are authorized for use.

## VI. Selective Placement Factors

### Optional Selective Factor

In **addition** to the proposed selective placement factors below, certifications/professional training may be added as per below:

Certification requirement. For IA – Position requires IA Category and Level certification.

Professional IT training, certifications/coursework in addition to experience related to the selective placement factor. For example, specialized IT certifications/coursework with various schools or vendors is continuing education (MSCE (certification), CISSP Certification Training or Certified Ethical Hacker (CEH) certification).



## Selective Placement Factors by Occupation

### 0391 Telecommunications

**GS 9:** Knowledge or skill in identifying security risks to implement and manage controls that ensure secure classified and unclassified communications as evidenced by education, training and/or experience.

**GS 11:** Knowledge or skill in identifying security risks to direct, control, implement and manage controls that ensure secure classified and unclassified communications as evidenced experience. Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; cyber incident response; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 12:** Knowledge or skill in identifying security risks to develop, evaluate, direct, control, implement and manage controls that ensure secure classified and unclassified communications as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; cyber incident response; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 13:** Knowledge or skill in identifying security risks to develop, evaluate, direct, control, implement and manage controls that ensure secure classified and unclassified communications as evidenced by experience. Ability to provide guidance in determining the most appropriate methods for delivering information securely via communications services.

Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; cyber incident response; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 14:** Knowledge and expertise in identifying security risks to develop, evaluate, direct, control, implement and manage controls that ensure secure classified and unclassified communications as evidenced by experience. Manage operations to determine the most appropriate methods for delivering information securely via communications services. Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; cyber incident response; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 15:** Mastery of security risks identification and determination and development of solutions to ensure secure classified and unclassified communications as evidenced by experience. Senior technical authority responsible for determination of the most



## Selective Placement Factors by Occupation

### **0391 Telecommunications (continued)**

appropriate methods for delivering information securely via communications services. Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; cyber incident response; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.



## Selective Placement Factors by Occupation

### **0854 – Computer Engineer**

GS-9: Knowledge and skills identifying cyber security computer engineering work involving the application of cyber security engineering and scientific theories and principles to complex cyber security computer-based systems. This position covers performance of professional cyber security engineering and scientific work involving the design, construction, and operation of cyber security computer systems, to include hardware and software and their integration. Specific cyber security knowledge and experience in one (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.

GS-11/12: Knowledge and skills identifying cyber security computer engineering work involving the application of cyber security engineering and scientific theories and principles to complex cyber security computer-based systems. This position covers performance of, and/or leading professional cyber security engineering and scientific work involving the design, construction, and operation of cyber security computer systems, to include hardware and software and their integration. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.

GS-13: Knowledge and skills identifying cyber security computer engineering work involving the application of cyber security engineering and scientific theories and principles to complex cyber security computer-based systems. This position covers leading, supervising, and/or performance of professional cyber security engineering and scientific work involving the design, construction, and operation of cyber security computer systems, to include hardware and software and their integration. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.



## Selective Placement Factors by Occupation

### **0854 – Computer Engineer (continued)**

GS-14/15: Knowledge and skills identifying cyber security computer engineering work involving the application of cyber security engineering and scientific theories and principles to complex cyber security computer-based systems. This position covers managing, supervising, leading, and/or performance of professional cyber security engineering and scientific work involving the design, construction, and operation of cyber security computer systems, to include hardware and software and their integration. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.



## Selective Placement Factors by Occupation

### **0855 – Electronics Engineer**

GS-9: Knowledge and skills identifying electronic engineering involves electronic circuits, circuit elements, equipment, systems, and associated phenomena concerned with electromagnetic or acoustical wave energy or electrical information for the purpose of cyber security. This series covers positions performing professional cyber security engineering and scientific work. Specific cyber security knowledge and experience in one (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis

GS-11/12: Knowledge and skills identifying electronic engineering involves electronic circuits, circuit elements, equipment, systems, and associated phenomena concerned with electromagnetic or acoustical wave energy or electrical information for the purpose of cyber security. This series covers positions performing and/or leading professional cyber security engineering and scientific work. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.

GS-13: Knowledge and skills identifying electronic engineering involves electronic circuits, circuit elements, equipment, systems, and associated phenomena concerned with electromagnetic or acoustical wave energy or electrical information for the purpose of cyber security. This series covers positions leading, supervising, and/or performing professional cyber security engineering and scientific work. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.

GS-14/15: Knowledge and skills identifying electronic engineering involves electronic circuits, circuit elements, equipment, systems, and associated phenomena concerned with electromagnetic or acoustical wave energy or electrical information for the purpose of cyber security. This series covers positions managing, supervising, leading, and/or performing professional cyber security engineering and scientific work. Specific cyber



## Selective Placement Factors by Occupation

### **0855 – Electronics Engineer (continued)**

security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.



## Selective Placement Factors by Occupation

### 1515 – Operations Research Analyst

GS-9: Knowledge and skills identifying this series covers positions that perform scientific cyber security work that involves designing, developing, and adapting mathematical, statistical, econometric, and other scientific methods and techniques. The work also involves analyzing management problems and providing advice and insight about the probable effects of alternative solutions to these problems. The primary requirement of the work is competence in the rigorous methods of scientific cyber security inquiry and analysis. Specific cyber security knowledge and experience in one (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis

GS-11/12: Knowledge and skills identifying this series covers positions that lead or perform scientific cyber security work that involves designing, developing, and adapting mathematical, statistical, econometric, and other scientific methods and techniques. The work also involves analyzing management problems and providing advice and insight about the probable effects of alternative solutions to these problems. The primary requirement of the work is competence in the rigorous methods of scientific cyber security inquiry and analysis. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.

GS-13: Knowledge and skills identifying this series covers positions that supervise, lead, or perform scientific cyber security work that involves designing, developing, and adapting mathematical, statistical, econometric, and other scientific methods and techniques. The work also involves analyzing management problems and providing advice and insight about the probable effects of alternative solutions to these problems. The primary requirement of the work is competence in the rigorous methods of scientific cyber security inquiry and analysis. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.



## Selective Placement Factors by Occupation

### **1515 – Operations Research Analyst (continued)**

GS-14/15: Knowledge and skills identifying this series covers positions that manage, supervise, lead, or perform scientific cyber security work that involves designing, developing, and adapting mathematical, statistical, econometric, and other scientific methods and techniques. The work also involves analyzing management problems and providing advice and insight about the probable effects of alternative solutions to these problems. The primary requirement of the work is competence in the rigorous methods of scientific cyber security inquiry and analysis. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.



## Selective Placement Factors by Occupation

### 1550 – Computer Scientist

GS-9: Knowledge and skills identifying computer scientists involve the development of new and improved cyber security concepts, principles, and techniques that will advance the body of knowledge of cyber security, and adapt and apply advanced cyber security computer science methods and techniques to solve complex cyber security computer processing requirements. Specific cyber security knowledge and experience in one (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis

GS-11/12: Knowledge and skills identifying computer scientists involve leading and/or performing in the development of new and improved cyber security concepts, principles, and techniques that will advance the body of knowledge of cyber security, and adapt and apply advanced cyber security computer science methods and techniques to solve complex cyber security computer processing requirements. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.

GS-13: Knowledge and skills identifying computer scientists involve supervising, leading, and/or performing in the development of new and improved cyber security concepts, principles, and techniques that will advance the body of knowledge of cyber security, and adapt and apply advanced cyber security computer science methods and techniques to solve complex cyber security computer processing requirements. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis.

GS-14/15: Knowledge and skills identifying computer scientists involve managing, supervising, leading, and/or performing in the development of new and improved cyber security concepts, principles, and techniques that will advance the body of knowledge of cyber security, and adapt and apply advanced cyber security computer science methods



## Selective Placement Factors by Occupation

### **1550 – Computer Scientist (continued)**

and techniques to solve complex cyber security computer processing requirements. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling and malware vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure inter-dependency analysis



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Policy and Planning**

**GS- 9:** Knowledge or skill identifying cyber security issues and risks to address future cybersecurity challenges as evidenced by education, training, and/or experience.

**GS-11:** Knowledge and skill identifying cyber security issues and risks and the ability to address future cyber security challenges as evidenced by experience. Specific cyber security knowledge and experience in one (or more) of the following areas required: cyber risk and strategic analysis; program management; incident handling; cyber incident response; cyber workforce structure and roles; education, training and exercise facilitation and management; enterprise architecture; and cyber-related infrastructure inter-dependency analysis.

**GS-12:** Knowledge and skill identifying cyber security issues and risks and the ability to develop strategies to address future cyber security challenges as evidenced by experience. Specific cyber security knowledge and experience in two (or more) of the following areas required: cyber risk and strategic analysis; program management; incident handling; cyber incident response; cyber workforce structure and roles; education, training and exercise facilitation and management; enterprise architecture; and cyber-related infrastructure inter-dependency analysis.

**GS-13:** Knowledge and skill in identifying cyber security issues and risks and the ability to develop policies, strategies, and guidance to address future cyber security challenges. The employee is recognized as a technical authority throughout the organization, and is responsible for implementing and integrating new programs or requirements and developing new policy, guidance, standards, and methods. Serves as expert for the organization, and analyzes and resolves difficult policy and planning problems or issues, conducts special studies, and makes recommendations on new approaches to delivering services. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling malware/vulnerability analysis; program management; distributed control systems security; cyber incident response; cyber exercise facilitation and management; cyber vulnerability detection and assessment; network and systems engineering; enterprise architecture; and, cyber-related infrastructure inter-dependency analysis.

**GS-14:** Knowledge and skill in identifying cyber security issues and risks and the ability to develop policies, strategies, and guidance to address future cyber security challenges. The employee is recognized as a technical authority throughout the organization, and is responsible for implementing and integrating new programs or requirements and developing new policy, guidance, standards, and methods. Serves as principal expert and manager for the organization, and analyzes and resolves difficult policy and planning problems or issues, manages special studies, and makes recommendations on new approaches to delivering services. Specific cyber security knowledge in two (or more) of



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Policy and Planning (continued)**

the following areas required: cyber risk and strategic analysis; incident handling malware/vulnerability analysis; program management; distributed control systems security; cyber incident response; cyber exercise facilitation and management; cyber vulnerability detection and assessment; network and systems engineering; enterprise architecture; and, cyber-related infrastructure inter-dependency analysis.

**GS-15:** Expertise and skill in identifying cyber security issues and risks and the ability to develop policies, strategies, and guidance to address future cyber security challenges. The employee is recognized as the senior technical authority throughout the organization, and is responsible for implementing and integrating new programs or requirements and developing new policy, guidance, standards, and methods. Serves as senior expert and leader for the organization, and analyzes and resolves difficult policy and planning problems or issues, manages one or more special studies, and makes recommendations on new approaches to delivering services. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling malware/vulnerability analysis; program management; distributed control systems security; cyber incident response; cyber exercise facilitation and management; cyber vulnerability detection and assessment; network and systems engineering; enterprise architecture; and, cyber-related infrastructure inter-dependency analysis.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Applications Software**

**GS 9:** Knowledge or skill in identifying software security risks to reduce risks as evidenced by education, training, and/or experience.

**GS 11:** Knowledge and skill in identifying software security risks and determining software solutions to reduce risks as evidenced by experience. Specific cyber security knowledge and experience in one (or more) of the following areas required: malware/vulnerability analysis; program management; distributed control systems security; cyber vulnerability detection and assessment; and cyber security software development.

**GS 12:** Knowledge and skill in identifying software security risks and determining/ developing software solutions to reduce risks as evidenced by experience. Specific cyber security knowledge and experience in two (or more) of the following areas required: malware/vulnerability analysis; program management; distributed control systems security; cyber vulnerability detection and assessment; and, cyber security software development.

**GS 13:** Knowledge and skill in software security design principles, methods, and approaches; principles, methods, and procedures for designing, developing, optimizing, and integrating new and/or reusable systems components; identifying software security risks to reduce risks as evidenced by education, training, and/or experience. Specific cyber security knowledge and experience in one (or more) of the following areas required: malware/vulnerability analysis; program management; distributed control systems security; cyber vulnerability detection and assessment; and, cyber security software development.

**GS 14:** Knowledge and expertise in identifying software security risks and determining software solutions to reduce risks as evidenced by experience. Manage teams to develop new work methods, standards, and practices designed to significantly improve the safety, quality, reliability, predictability, reusability, and cost performance of applications software systems. Specific cyber security knowledge and experience in one (or more) of the following areas required: malware/vulnerability analysis; program management; distributed control systems security; cyber vulnerability detection and assessment; and, cyber security software development.

**GS 15:** Mastery of systems security engineering concepts and factors, such as structured design; supportability; survivability; reliability; scalability; and maintainability sufficient to ensure that applications are optimized for state-of-the-art technology and functionality as evidenced by education, training, and/or experience. Senior technical authority responsible for standards, and practices designed to significantly improve the safety, quality, reliability, predictability, reusability, and cost performance of applications software systems. Specific cyber security knowledge and experience in two (or more) of the following areas required: malware/vulnerability analysis; program management; distributed control systems security; cyber vulnerability detection and assessment; and, cyber security software development.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Customer Support**

**GS 9:** Knowledge or skill in determining network and application cybersecurity incidents, type of incident, and initial incident response as evidenced by education, training, and/or experience.

**GS 11:** Knowledge and skill in determining network and application cyber security incidents, type of incident, and initial incident response as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: incident handling and malware/vulnerability analysis, and cyber incident response.

**GS 12:** Knowledge and skill in determining network and application cyber security incidents, type of incident, and initial incident response as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: incident handling and malware/vulnerability analysis, and cyber incident response.

**GS 13:** Knowledge and skill in determining network and application cybersecurity incidents, type of incident, and initial incident response as evidenced by education, training, and/or experience. Specific cyber security knowledge in one (or more) of the following areas required: incident handling and malware/vulnerability analysis, and cyber incident response.

**GS 14:** Knowledge and expertise in determining and managing network and application cyber security incidents, type of incident, and initial incident response as evidenced by education, training, and/or experience. Manage teams to plan and deliver a full range of customer support services to the organization and to install, configure, upgrade, and troubleshoot hardware and software components. Specific cyber security knowledge in one (or more) of the following areas required: incident handling and malware/vulnerability analysis, and cyber incident response.

**GS 15:** Mastery of processes and procedures required to leading efforts to address network and application cyber security incidents, types of incident, and initial incident response as evidenced by education, training, and/or experience. Senior technical authority responsible for planning and delivery of a full range of customer support services to the organization and install, configure, upgrade, and troubleshoot any hardware and software components. Specific cyber security knowledge in one (or more) of the following areas required: incident handling and malware/vulnerability analysis, and cyber incident response.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Data Management**

**GS 9:** Knowledge or skill in identifying security risks to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data; and reduce risks as evidenced by education, training, and/or experience.

**GS 11:** Knowledge and skill in identifying security risks and determining solutions to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data; and reduce risks as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: malware/vulnerability analysis; distributed control systems security; cyber vulnerability detection and assessment; incident handling and cyber incident response.

**GS 12:** Knowledge and skill in identifying security risks and determining and developing solutions to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data; and reduce risks as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: malware/ vulnerability analysis; distributed control systems security; cyber vulnerability detection and assessment; incident handling and cyber incident response.

**GS 13:** Knowledge and skill in identifying security risks to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data; and reduce risks as evidenced by education, training, and/or experience. Ability to apply cybersecurity concepts in the design, development, and maintenance of data management systems and databases. Specific cyber security knowledge in one (or more) of the following areas required: malware/vulnerability analysis; distributed control systems security; cyber vulnerability detection and assessment; incident handling and cyber incident response.

**GS 14:** Knowledge and expertise in identifying security risks to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data; and reduce risks as evidenced by education, training, and/or experience. Manage teams to ensure inclusion of cybersecurity concepts in the design, development, and maintenance of data management systems and databases. Specific cyber security knowledge in one (or more) of the following areas required: malware/vulnerability analysis; distributed control systems security; cyber vulnerability detection and assessment; incident handling and cyber incident response.

**GS 15:** Mastery of security risks identification and determination and development of solutions to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data; and reduce risks as evidenced by as evidenced by education, training, and/or experience. Senior technical authority responsible for inclusion of cybersecurity concepts in the design, development, and maintenance of data management systems and databases. Specific cyber security knowledge in two (or more) of the following areas required: malware/ vulnerability analysis; distributed control systems security; cyber vulnerability detection and assessment; incident handling and cyber incident response.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Internet**

**GS 9:** Knowledge or skill in identifying security risks to ensure the availability, integrity, and confidentiality of Internet, intranet, and extranet services as evidenced by education, training, and/or experience.

**GS 11:** Knowledge and skill in identifying security risks and determining solutions to ensure the availability, integrity, and confidentiality of Internet, intranet, and extranet services as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis, and cyber incident response.

**GS 12:** Knowledge and skill in identifying security risks and determining and developing solutions to ensure the availability, integrity, and confidentiality of Internet, intranet, and extranet services as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: distributed control systems security; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis, and cyber incident response.

**GS 13:** Knowledge or skill in identifying security risks to ensure the availability, integrity, and confidentiality of Internet, intranet, and extranet services as evidenced by education, training, and/or experience. Ability to provide guidance in determining the most appropriate methods for delivering information via the Internet, creation of Internet applications, and management of Internet resources. Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis, and cyber incident response.

**GS 14:** Knowledge and expertise in identifying security risks to ensure the availability, integrity, and confidentiality of Internet, intranet, and extranet services as evidenced by education, training, and/or experience. Manage teams to determine the most appropriate methods for delivering information via the Internet; creation of Internet applications; and management of Internet resources. Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis, and cyber incident response.

**GS 15:** Mastery of security risks identification and determination and development of solutions to ensure the availability, integrity, and confidentiality of Internet, intranet, and extranet services as evidenced by education, training, and/or experience. Senior technical authority responsible for determination of the most appropriate methods for delivering information via the Internet, creation of Internet applications, and management of Internet resources. Specific cyber security knowledge in one (or more) of the following areas required: distributed control systems security; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis, and cyber incident response.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Network Services**

**GS 9:** Knowledge or skill in identifying security risks to integrate security solutions into the design, development, configuration, integration and management of networks as evidenced by education, training, and/or experience.

**GS 11:** Knowledge and skill in identifying security risks and determine and promulgate solutions to integrate security solutions into the design, development, configuration, integration and management of networks as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; cyber incident response; and, cyber-related infrastructure inter-dependency analysis.

**GS 12:** Knowledge and skill in identifying security risks and determine/develop/promulgate solutions to integrate security solutions into the design, development, configuration, integration and management of networks as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; cyber incident response; and, cyber-related infrastructure inter-dependency analysis.

**GS 13:** Knowledge or skill in identifying security risks to integrate security solutions into the design, development, configuration, integration and management of networks as evidenced by education, training, and/or experience. Ability to provide guidance in the areas of network systems design, development, testing, installation, integration, operations, management, and maintenance. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; cyber incident response; and, cyber-related infrastructure inter-dependency analysis.

**GS 14:** Knowledge and expertise in identifying security risks to integrate security solutions into the design, development, configuration, integration and management of networks as evidenced by education, training, and/or experience. Manage teams to design, development, test, install, integrate, operate, manage, and maintain network systems. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; cyber incident response; and, cyber-related infrastructure inter-dependency analysis.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Network Services (continued)**

**GS 15:** Mastery of security risks identification and determination and development of solutions to ensure security solutions integration into the design, development, configuration, integration and management of networks as evidenced by education, training, and/or experience. Senior technical authority responsible for the design, development, testing, installation, integration, operation, management, and maintenance of network systems. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; cyber incident response; and, cyber-related infrastructure inter-dependency analysis.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Operating Systems**

**GS-9:** Knowledge or skill in identifying security risks to integrate security solutions into the design, development, configuration, integration and management of operating systems as evidenced by education, training, and/or experience.

**GS-11:** Knowledge and skill in identifying security risks and determine and promulgate solutions to integrate security solutions into the design, development, configuration, integration and management of operating systems as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.

**GS 12:** Knowledge and skill in identifying security risks and determine/develop/promulgate solutions to integrate security solutions into the design, development, configuration, integration and management of operating systems as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.

**GS-13:** Knowledge or skill in identifying security risks to integrate security solutions into the design, development, configuration, integration and management of operating systems as evidenced by education, training, and/or experience. Ability to provide guidance in the areas of operating systems design, development, testing, installation, integration, operation, management, and maintenance. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.

**GS-14:** Knowledge and expertise in identifying security risks and determine and promulgate solutions to integrate security solutions into the design, development, configuration, integration and management of operating systems as evidenced by education, training, and/or experience. Manage teams to design, development, test, install, integrate, operate, manage, and maintain operating systems. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Operating Systems (continued)**

assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.

**GS 15:** Mastery of security risks identification and determination and development of solutions to integrate security solutions into the design, development, configuration, integration and management of operating systems. Senior technical authority responsible for the design, development, testing, installation, integration, operation, management, and maintenance of operating systems. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Project Management**

**GS-9:** Knowledge or skill in identifying security risks to integrate security solutions into the design, development, configuration, integration and management of Information technology product, service or system acquisition as evidenced by education, training, and/or experience.

**GS-11:** Knowledge and skill in identifying security risks and determining and promulgating solutions to integrate security solutions into the design, development, configuration, integration and management of Information technology product, service or system acquisition as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS-12:** Knowledge and skill in identifying security risks and determining/developing/promulgating solutions to integrate security solutions into the design, development, configuration, integration and management of Information technology product, service or system acquisition as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS-13:** Knowledge or skill in integration security solutions into the design, development, configuration, testing, integration and management of Information Technology products, services or system acquisitions as evidenced by education, training, and/or experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS-14:** Knowledge and expertise in identifying security risks and determining and promulgating solutions to integrate security into the design, development, configuration, testing, integration and management of Information technology product, service or system acquisition as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Project Management (continued)**

assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS-15:** Mastery of security risks identification and determination and development of solutions to integrate security into the design, development, configuration, testing, integration and management of Information technology product, service or system acquisition as evidenced by experience. Senior technical authority responsible for the design, development, testing, installation, and integration Information technology acquisitions. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Security**

**GS 9:** Knowledge or skill in identifying security risks to integrate security solutions into the design, development, configuration, integration and management of operating systems as evidenced by education, training, and/or experience.

**GS 11:** Knowledge and skill in identifying security risks and determining and promulgating solutions to integrate security solutions into the design, development, configuration, integration and management of operating systems as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; training and exercise facilitation and management; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 12:** Knowledge or skill in identifying security risks and determining/developing/promulgating solutions to integrate security solutions into the design, development, configuration, integration and management of operating systems as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; training and exercise facilitation and management; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 13:** Knowledge and skill in implementation, operation and management of security programs designed to anticipate, assess, and minimize system vulnerabilities as evidenced by education, training, and/or experience. Ability to develop, implement, maintain, operate and enhance information systems security programs, policies, procedures, and tools. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; incident handling malware/vulnerability analysis; program management; distributed control systems security; cyber incident response; cyber exercise facilitation and management; cyber vulnerability detection and assessment; network and systems engineering; enterprise architecture; and, cyber-related infrastructure inter-dependency analysis.

**GS 14** Knowledge and skill in implementation, operation and management of security programs designed to anticipate, assess, and minimize system vulnerabilities as evidenced by education, training, and/or experience. Manage teams to develop, implement, maintain, operate and enhance information systems security programs, policies, procedures, and tools. Specific cyber security knowledge in two (or more) of the



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Security (continued)**

following areas required: cyber risk and strategic analysis; incident handling malware/vulnerability analysis; program management; distributed control systems security; cyber incident response; cyber exercise facilitation and management; cyber vulnerability detection and assessment; network and systems engineering; enterprise architecture; and, cyber-related infrastructure inter-dependency analysis .

**GS 15:** Mastery of security risks identification and determination and development of solutions to integrate security into the design, development, and implementation of security programs, policies, procedures, and tools as evidenced by education, training, and/or experience. Senior technical authority responsible for applying systems security principles, methods, regulations, and policies to meet security requirements. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and cyber-related infrastructure inter-dependency.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Systems Administration**

**GS 9:** Knowledge or skill in identifying security risks to ensure the availability, integrity, and confidentiality of IT systems as evidenced by education, training, and/or experience.

**GS 11:** Knowledge and skill in identifying security risks and determining and promulgating solutions to ensure the availability, integrity, and confidentiality of IT systems as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.

**GS 12:** Knowledge and skill in identifying security risks and determining/developing/promulgating solutions to ensure the availability, integrity, and confidentiality of IT systems as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.

**GS 13:** Knowledge or skill in identifying security risks to ensure the availability, integrity, and confidentiality of IT systems as evidenced by education, training, and/or experience. Ability to manage multi-user computing environment(s), install and configure system hardware and software, manage and monitor system access, upgrade software and conduct backup and recovery. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.

**GS 14:** Knowledge and expertise in identifying security risks and determining and promulgating solutions to ensure the availability, integrity, and confidentiality of IT systems as evidenced by experience. Manage teams to manage multi-user computing environment(s), install and configure system hardware and software, manage and monitor system access, upgrade software and conduct backup and recovery. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Systems Administration (continued)**

**GS 15:** Knowledge and skill in identifying security risks and determining/developing/promulgating solutions to ensure the availability, integrity, and confidentiality of IT systems as evidenced by experience. Senior technical authority responsible for multi-user computing environment(s), installation and system hardware and software configuration, system access management and monitoring, software upgrade and backup and recovery processes and operations. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber incident response.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Systems Analysis**

**GS 9:** Knowledge of or skill in identifying and analyzing security risks to integrate security solutions into the design, development, configuration, integration and management of information systems as evidenced by education, training, and/or experience.

**GS 11:** Knowledge and skill in identifying and analyzing security risks and determining and promulgating solutions to integrate security solutions into the design, development, configuration, integration and management of information systems as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 12:** Knowledge and skill in identifying and analyzing security risks and determining/developing/promulgating solutions to integrate security solutions into the design, development, configuration, integration and management of information systems as evidenced by experience. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and cyber-related infrastructure inter-dependency.

**GS 13:** Knowledge of or skill in identifying and analyzing security risks to integrate security solutions into the design, development, configuration, integration and management of information systems as evidenced by education, training, and/or experience. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 14:** Knowledge and skill in identifying and analyzing security risks and determining and promulgating solutions to integrate security solutions into the design, development, configuration, integration and management of information systems as evidenced by education, training, and/or experience.. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.



## Selective Placement Factors by Occupation

### **2210 IT Specialists: Parenthetical – Systems Analysis (continued)**

**GS 15:** Mastery of security risks identification and determination and development of solutions to integrate security into the design, development, configuration, integration and management of information systems as evidenced by education, training, and/or experience. Ability to develop Enterprise Architecture artifacts. Senior technical authority responsible for new systems design methodologies software development risk determination; and determination of the impact of new systems design policies on the systems design process. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and cyber-related infrastructure inter-dependency.



## Selective Placement Factors by Occupation

### **GS-2210 - Parenthetical – Enterprise Architecture**

**GS 9:** Knowledge or skill in identifying security risks to integrate security solutions into the enterprise architecture framework as evidenced by education, training and/or experience.

**GS 11:** Knowledge or skill in identifying security risks to integrate security solutions into the enterprise architecture framework as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: enterprise architecture; distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 12:** Knowledge or skill in identifying security risks and determining, developing, and incorporating security solutions into the enterprise architecture framework as evidenced by experience. Specific cyber security knowledge in one (or more) of the following areas required: enterprise architecture; distributed control systems security; network and systems engineering; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 13:** Knowledge or skill in identifying and analyzing security risks to integrate security solutions into the enterprise architecture framework to integrate security strategies, plans, standards, and principles into mission, goals, and business processes of the organization as evidenced by education, training, and/or experience. Ability to develop Enterprise Architecture plans, artifacts, reference models, and standards. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.

**GS 14:** Knowledge or skill in identifying and analyzing security risks to integrate security solutions into the enterprise architecture framework to integrate security strategies, plans, standards, and principles into mission, goals, and business processes of the organization as evidenced by education, training, and/or experience. Manage teams to develop Enterprise Architecture plans, artifacts, reference models, and standards. Specific cyber security knowledge in one (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and, cyber-related infrastructure inter-dependency.



## Selective Placement Factors by Occupation

### **GS-2210 - Parenthetical – Enterprise Architecture (continued)**

**GS 15:** Mastery of security risks identification and determination and development of solutions to integrate security into the design, development, configuration, integration and management of information systems as evidenced by education, training, and/or experience. Senior technical authority responsible for Enterprise Architecture plans, artifacts, reference models, and standards. Specific cyber security knowledge in two (or more) of the following areas required: cyber risk and strategic analysis; enterprise architecture; program management; distributed control systems security; network and systems engineering; enterprise architecture; cyber vulnerability detection and assessment; incident handling and malware/vulnerability analysis; and cyber-related infrastructure inter-dependency.



## VII. Hiring Methodology

This establishes hiring procedures for the use of this authority. There are two methods for hiring using this authority: a streamlined approach or using a vacancy announcement to solicit candidates. There is no requirement for a vacancy announcement, but managers may wish to post an individual announcement. Additionally, commands may market their vacancies using a flyer and have the flyer direct candidates to apply to one of the open continuous announcements created for the Cyber Security Workforce. Currently we have prepared and have available for use the GS-2210, GS-854, and GS-855 announcement templates. Managers are encouraged to work with their HRO and HRSC to implement a recruitment plan that best suits their needs. Merit System principles and veterans preferences entitlements will be afforded as contained in 5 CFR 302.

Using the streamlined (Name Request) is simple. A Selecting officials or SMEs may identify a candidate through a “name request”. The following steps are provided:

### **What to include with the RPA for a Name Request**

1. PD—with standard paragraphs for Cyber Security to indicate that these are Cyber Security Workforce Excepted Service positions
2. Selective Placement Factors
3. Resume
4. Transcripts (if positive education required)
5. OF 306
6. Notepad: Schedule A appointing authority 213.3106(b)(11) and include how the Selective Placement was met

Using the traditional method of announcing the position may take longer but may solicit a larger number of candidates. The following steps are provided:

### **What to include with a Recruit/Fill RPA**

1. PD—with standard paragraphs for Cyber Security to indicate that these are Cyber Security Workforce Excepted Service positions
2. Appropriate Selective Placement
3. Notepad: Identify the Recruitment Sources that hiring manager wants to consider (Individual announcement, OCA created for Cyber community (must be 855, 854 or 2210), Schedule A appointing authority 213.3106(b)(11), Required Selective Placement factor

## VIII. Positions in Alternative Personnel Systems

Those positions in alternative personnel systems are eligible for appointment using the Schedule A appointing authority based on OPM memo dtd 5/3/2010. The use of selective placement factors will be done in the same manner as current methodology for qualifications determinations (e.g., YA-2 under positions will use the GS-9 Selective Placement Factor).



## IX. DCPDS Coding

There is no separate DCPDS Code for these hires.

Use Authority Code XZM; Authority 213.3106(b) (11); Event Code: LS12004

**X. Allocations:** As distributed below. \*\*Fifteen billets held in SECNAV reserve.

USMC	SPAWAR	AIR	RES	NETWAR COM	NAVSEC WARCOM	MSC	NAVSEA	USFFC	NETC	CNIC	CYBER	NCIS	**Total
400	215	1	1	300	3	19	6	7	2	5	19	20	998

## XI. Reporting

Major commands, working with the HRSCs, will provide OCHR quarterly input beginning July 15, 2010, on the number of positions filled using this authority; the pay plan, occupation, series, and grade (or equivalent) of the position; and the nature of action of each hire. OCHR will forward a data call to ascertain this information each quarter.

### Appendix A: References

- a. OPM memo of May 3, 2010
- b. CPMS memo of Mar 25, 2010
- c. CMPS memo of Nov 27, 2009
- d. OPM memo of Nov 10, 2009



# Appendix A

## References:

- a. OPM memo of May 3, 2010
- b. CPMS memo of Mar 25, 2010
- c. CMPS memo of Nov 27, 2009
- d. OPM memo of Nov 10, 2009