Ms. Marilee Fitzgerald  
Acting Deputy Under Secretary  
Civilian Personnel Policy  
Office of the Under Secretary of Defense  
4000 Defense Pentagon  
Washington, DC 20301-4000

Dear Ms. Fitzgerald:

I am providing an updated copy of the Schedule A authority to staff certain positions for a cyber security workforce within the Department of Defense (DoD). As approved, the Schedule A authority reads as follows:

Section 213.3106(b) Department of Defense  
(11) Not to exceed 3000 positions that require unique cyber security skills and knowledge to perform 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. This authority may be used to make permanent, time-limited and temporary appointments in the following occupational series: Security (GS-0080), intelligence analysts (GS-0132), computer engineers (GS-0854), electronic engineers (GS-0855), computer scientists (GS-1550), operations research (GS-1515), criminal investigators (GS-1811), telecommunications (GS-0391), and IT specialists (GS-2210). Within the scope of this authority, the U.S. Cyber Command is also authorized to hire miscellaneous administrative and program (GS-0301) series when those positions require unique cyber security skills and knowledge. All positions will be at the General Schedule (GS) grade levels 09-15 or equivalent. No new appointments may be made under this authority after December 31, 2012.

If you have any questions, please contact Gale Perryman at 202-606-1143.

Sincerely,

[Signature]

Michael J. Mahoney  
Manager, Hiring Policy
MEMORANDUM FOR DIRECTOR, PERSONNEL POLICY, DEPARTMENT OF THE AIR FORCE

MAR 25 2010

SUBJECT: Schedule A Hiring Authority for the Cyber Security Workforce

This memorandum responds to your request for authority to fill cyber security positions covered by the enclosed Office of Personnel Management (OPM) memorandum.

The authority is Department of Defense (DoD) wide but is limited to a specific number of positions, not to exceed 3000 allocations Department-wide.

Since the authority is limited to a specific number of positions, allocations are set based on projected need. The Department of the Air Force (AF) is authorized to fill 683 new and existing cyber security positions.

The AF is responsible for assigning allocations to organizations under your purview and ensuring the allocations are not exceeded. If you are not going to utilize your total allocations or if the need arises for additional ones, please notify us so that appropriate adjustments can be made.

Authority is limited to the series listed in the attached OPM approval memorandum and only applies to positions that justify the use of a selective placement factor for unique cyber security skills and knowledge. When making appointments, the DoD Schedule A authority 213.3106(b)(11) must be cited as the authority and you must use the excepted hiring procedures found in 5 CFR part 302.

Should you have any questions regarding the use of this authority, my point of contact for this action is Mr. Johnny McLean, Chief, Field Advisory Services. He can be reached at (703) 696-1615.

Sharon Stewart
Acting Director

Attachment:
As stated
Section 1A – Overview

Hiring Process Overview. This instruction establishes procedures for filling cyber security workforce vacancies under the Schedule A authority granted to the Department of Defense (DoD) by the Office of Personnel Management under 5 CFR 213.3106(b)(11). Under this authority, 683 cyber security workforce positions have been allocated to the Department of the Air Force for USSTRATCOM, 24th Air Force, and AFOSI positions requiring unique qualifications to perform: 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 interdependency analysis. USSTRATCOM, 24th Air Force and AFOSI have been given a specific number of authorizations that may be filled using this authority. Allocations may not be exceeded.

Appointments may be made as permanent, time-limited, or temporary. Positions will be at General Schedule (GS) grade levels 09-15. No new appointments may be made under this authority after December 31, 2012 or the date on which OPM establishes applicable qualification standards, whichever is earlier.

Series that are currently covered under this authority specifically include: Security (GS-0080), Intelligence Analysts (GS-0132), Telecommunications (GS-0391), Computer Engineers (GS-0854), Electronic Engineers (GS-0855), Operations Research (GS-1515), Computer Scientists (GS-1550), Criminal Investigators (GS-1811), and IT specialists (GS-2210). The Planner (GS-0301) series is provided for USCYBERCOM use only.

1.1. Hiring Process. The hiring process begins when you create a new position and complete the position description classification, or when incumbents announce their intent to leave.

1.1.1. The office having the vacancy submits a request to the servicing civilian personnel office to get the position filled by completing an SF 52, Request for Personnel Action.

1.1.2. The civilian personnel office prepares an examination announcement and starts the recruitment process. The announcement is left open for at least five days (often longer, depending on the position, location and skills required). When the applications are received, they are ranked by the servicing civilian personnel office against qualifications standards in accordance with the selective placement factors (Attachment 1).

1.1.3. A certificate of eligibles of qualified candidates is forwarded to the selecting official to complete the recruitment process (review of resumes, interview, etc.).

Section 1B – Roles, Responsibilities and Procedures

1.2. Selecting Official. The selecting official is responsible for evaluating applicants based on experience, education and other qualifications as required by the qualification requirements approved for the position which is being filled.

1.2.1. Veterans’ Preference. The principle of veterans’ preference shall be followed in accordance with 5 CFR 302.

1.2.2. Oral Interview. If interview is desired, after initially ranking the applications, the selecting official will normally notify the three best qualified candidates to appear for an interview. Circumstances may dictate more or fewer interviews. In the event a candidate resides outside the local area and cannot travel to participate in a live interview, the interview may be conducted by telephone.
1.3. **Civilian Personnel Office.** In making appointments under the provisions of this authority, the civilian personnel office has the following responsibilities:

1.3.1. Verify that the position is a cyber security position covered by the DoD Civilian Personnel Management Service (CPMS) memorandum dated November 27, 2009 and suitable qualification requirements are established.

1.3.2. Recruit qualified candidates in sufficient numbers to enable selection of the best available person.

1.3.3. Prepare recruitment notices and obtain completed forms and supporting data for use in the appointment process. A vacancy announcement prepared by the civilian personnel office constitutes the recruitment notice.

   1.3.3.1. The announcement will clearly define that the position being advertised is in the Excepted Service and does not confer competitive service eligibility.

   1.3.3.2. Ordinarily, the closing date should not be set to fall on a weekend or holiday.

   1.3.3.3. Applications received after the closing date are not accepted.

1.3.4. Determine that applicants meet all requirements for appointment.

1.3.5. Comply with veterans’ preference requirements.

1.3.6. Furnish the selecting official with the certificate of eligibles who have been examined and rated.

1.3.7. Process the personnel action after the requirements of this instruction have been met.
ACCELERATED PROCEDURES FOR CYBER SECURITY
POSITIONS UNDER SCHEDULE A AUTHORITY

Section 2A – Overview

2.1. Filling Vacancy Without Further Recruitment. Whenever any cyber security Schedule A authority vacancy occurs for which one or more known, qualified, and interested candidate exists, such vacancy may be filled without further recruitment and public notice.

2.1.1. This section establishes procedures which contemplate:

2.1.1.1. Knowledge of one or more qualified, interested candidate for a vacancy.

2.1.1.2. The need for rapid response to take advantage of the opportunity to hire such person(s).

2.2. Streamlined Process. These procedures eliminate the announcement, formal recruitment, and pre-screening phases of the recruitment process. The evaluation process is thus shortened by limiting the number of candidates that must be reviewed and interviewed.

Section 2B – Candidate Files

2.3. Candidate Files. Hiring officials are encouraged to maintain current files of qualified candidates (in-house or otherwise) for the types and levels of cyber security positions in the organization. This helps managers to fill rapidly when critical vacancies arise.

Section 2C – Roles, Responsibilities and Procedures

2.4. Roles, Responsibilities and Procedures. When an office having a cyber security vacancy knows of one or more qualified candidate that is interested in the job, the following procedures may be substituted for those set forth in Section 1.

2.4.1. The selecting official having the vacancy shall submit the name of the candidate to the servicing civilian personnel office with the position description, resume and SF 52 for review and initiation of fill action.

2.4.2. The civilian personnel office verifies that the position to be filled is a cyber security Schedule A position and qualification requirements are established.

2.4.3. The civilian personnel office reviews resume for completeness and satisfaction of qualifications.

2.4.4. The civilian personnel office ensures compliance with veterans’ preference requirements.

2.4.5. The civilian personnel office prepares a decision notification to the selecting official.

2.4.6. The civilian personnel office processes the personnel action after the requirements of this instruction have been met.
The interim qualification requirements outlined herein are established as supplements to existing OPM qualification requirements and must be used when filling positions covered by this Schedule A authority within the DoD. The intent of these interim qualification requirements is to outline the minimum requirements that are necessary for entry into positions that perform critical functions in a cyber security environment.

These standards refine and/or expand requirements established by the OPM Qualification Standards and outline the skill(s) that is/are:

- essential for successful performance on the job;
- geared toward a specific technical competency/knowledge, skill, or ability related to cyber security;
- require extensive training or experience to develop; and
- cannot be learned on the job in a reasonable amount of time.

The sample specialized experience statements included in this document are just that - samples. Other experience may be identified within the specialized experience statement when recruiting, based on the needs of position being filled. The selective factors, however, do constitute "screen outs" - all candidates will be required to have the ability identified in the selective factor, in addition to what's required by the OPM qualification standard (e.g., education requirements).

Security Specialist, GS-0080

Selective Factor: Ability to develop and implement cyberspace policies, procedures, standards, training, and/or methods used to identify and protect information, personnel, property, facilities, operations, and/or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss for operations in order to operate network and information systems, as well as protect, detect, and/or mitigate information technology (IT) vulnerabilities.

Sample Specialized Experience:
- Analyzing and resolving complex facility safety or security problems;
- Developing and managing security contingency plans and annexes;
- Coordinating and conducting vulnerability assessments, incorporating the assessment data into contingency plans and the development of emergency practice exercises;
- Providing guidance regarding the implementation of security guidelines at lower levels;
- Recommending and implementing policies, procedures, and methods for identifying and protecting people, property, operations, and material;
- Developing, coordinating and participating in security exercises.

Intelligence Specialist, GS-0132

Selective Factor: Ability to analyze threats to computer systems and networks, such as analysis of computer and network incidents, attribution of malicious network activity, and/or adversary network analysis, using intelligence analysis methodologies in order to support the operation, protection, and defense of critical networks and systems.

Sample Specialized Experience:
- Performing intelligence analysis and collection management tasks relating to cyberspace operations using state of the art intelligence methods;
• Collecting, evaluating, interpreting, and integrating data from multiple sources concerning the relevance and significance of developments/technical information related to cyber-security threats;
• Conducting joint analysis of mutual cyber-security intelligence problems and production efforts with other organizations involved in cyber-security related intelligence functions;
• Identifying cyber related intelligence gaps and specifying collection requirements to fill those gaps; writing and reviewing cyber intelligence analyses or assessments, briefings, studies, estimates, and evaluations;
• Developing analytical tools, methodologies, and other products (e.g., data bases, studies, estimates) supporting cyber analysis;
• Reviewing intelligence products prepared by other government agencies for technical accuracy and appropriate treatment and interpretation of information;
• Representing the organization/agency on related panels, committees, meetings and conferences dealing with threats to computer network operations and cyber-security;
• Identifying intelligence gaps and specifying collection requirements to fill gaps; writing and reviewing intelligence analyses or assessments, briefings, studies, estimates, and evaluations;
• Developing analytical tools, methodologies, and other products (e.g., data bases, studies, estimates);
• Reviewing intelligence products prepared by other government agencies for technical accuracy and appropriate treatment and interpretation of information;
• Representing the organization/agency on related panels, committees, meetings and conferences dealing with computer network operations and cyber-security.

Planner, GS-0301

Selective Factor: Ability to conduct military/contingency and crisis action planning for cyberspace operations in order to operate network and information systems, as well as protect, detect, and/or mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:
• Performing analysis of complex military operations to include force management, mobilization, deployment, logistics, readiness, homeland security, force integration, and training using mathematical, statistical, computer tools, simulation, and other scientific methods or techniques.
• Determining realistic assumptions, requirements for data, specific analytical approaches and other analytic techniques to be used in military operations planning (adaptive and crisis action) and execution;
• Performing analysis with models, simulations, and analytical tools/methods with a high degree of success;
• Providing technical coordination and advice to organizational staff/contractors on Joint and Service analytical requirements, projects and methodology;
• Documenting and tracking status of projects including functional use, technical specifications and resource implications;
• Applying a broad range of experience and knowledge of Federal, as well as Department of Defense (DoD), policies, procedures and processes in order to plan, develop, coordinate, implement, manage, and support analytical requirements;
• Utilizing detailed understanding of the principles inherent in military operations planning to envision, coordinate, or develop decision support solutions for staff and management;
• Applying working knowledge of current developments in operations research and computer simulation applications;
• Serving as technical director/interface and/or project manager of analysis, modeling and simulation contractors and evaluates validity of products to accomplish required capabilities in support of military missions and functions.

Telecommunication Specialist, GS-0391

Selective Factor: Ability to operate telecommunications systems, and network/information systems, as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Revised 14 May 2010
Sample Specialized Experience:

- Planning and directing the design, development, and implementation of network systems;
- Developing, planning, and implementing the overall strategic goals of organizational telecommunications network systems;
- Evaluating and recommending changes to current and future network requirements to meet the organizational needs;
- Ensuring daily security, operational, and maintenance support of worldwide and local personnel area networks;
- Monitoring fault, performance, configuration, and security management on network devices for assigned installations for a large, geographically dispersed organization;
- Providing network and systems management support to ensure end-user and organizational information systems service requirements are satisfied;
- Monitoring network activity throughout a large, geographically dispersed organization for selected systems and configurations;
- Administering guidance and direction, ensuring critical problems are evaluated and resolved quickly and efficiently;
- Ensuring network analysis, network design, and network installation are performed in support of worldwide personnel functions;
- Advising and briefing superiors on sensitive policy issues and problems, making recommendations in critical areas, and initiating authoritative professional action, as necessary, to eliminate cyber threat and system vulnerability.

Computer Engineer, GS-0854

Selective Factor: Ability to evaluate state-of-the-art scientific and engineering technologies and incorporating into the planning, design, operation, maintenance, repair, and upgrade of IT and communication systems in order to operate network and information systems, as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:

- Performing professional computer engineering work, including directing or managing enterprise programs involving cyber vulnerability detection and assessment; network and systems engineering; and cyber enterprise architecture;
- Plans, prioritizes, and advocates for requirements in the area of Technical Assurance (TA) Evaluations;
- Oversees the development of TA standards to determine any shortcomings;
- Performing positive functional testing and anti-forensics testing to determine any capability shortcomings, making recommendations to developers to mitigate shortcoming;
- Providing authoritative technical decisions, advice, and consultation affecting various aspects of computer network operations;
- Serving as a senior expert and consultant to management officials on IT architectural modeling and planning used in IT program integration, cyber risk and strategic analysis.

Electronics Engineer, GS-0855

Selective Factor: Ability to conduct systems modeling, simulation and testing, system requirements analysis, and advanced design synthesis, applying analysis of radio frequency (RF) electromagnetic spectrum properties, electromagnetic wave principles, and electromagnetic environmental effects in order to operate network and information systems as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:

- Applying electronics engineering concepts, principles and methods applicable to varied computer network security problems, projects, or studies that involve system/network design and/or development;
- Modifying standard practices, adapting precedents, and making departures from existing approaches and techniques;
- Overseeing system technical designs and system vulnerability analyses;
- Performing studies of system and equipment failures and developing failure trends of systems and subassemblies;
- Performing equipment and system life cycle studies and analyses.

**Computer Scientist, GS-1550**

Selective Factor: Ability to conduct comprehensive network and information system technology analysis, design, programming, verification, risk planning, and/or life cycle support in an IT environment in order to operate network and information systems as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:
- Designing, developing, and fielding systems/materiel that support mission requirements, ensuring systems/materiel are equipped with security measures commensurate with their criticality to overall mission;
- Serving as a technical subject matter expert, providing analytical and technical advice to support and defend major principle policy and business decisions in the areas of information assurance and security, operational net-centric readiness, theoretical modeling, performance measures, high performance computing techniques, planning, and forecasting methods;
- Applying and integrating advanced IA and IT security within the Component information policy structure for organizations and programs requiring special access controls;
- Advising and briefing advanced IT security within the Component information policy structure for organizations and programs requiring special access controls;
- Advising and briefing superiors on sensitive policy issues and problems, making recommendations in critical areas, and initiating authoritative professional action, as necessary, to eliminate cyber threat and system vulnerability.

**Operations Research Analyst, GS-1515**

Selective Factor: Ability to design, develop, adapt, and/or apply decision-making models related to information security in a cyberspace IT environment in order to operate network and information systems as well as protect, detect, and mitigate IT vulnerabilities.

Sample Specialized Experience:
- Conducting vulnerability analyses of cyber operations and systems;
- Gathering, compiling and organizing quantitative data using computer systems and software applications;
- Reviewing and assimilating data from various test and evaluation documents/inputs;
- Generating risk analysis reports to aid senior management in determining whether a particular CNA capability should be employed, based on its potential risk and unintended consequences;
- Formulating quantitative cyber-security solutions;
- Writing draft technical reports on routine or noncomplex research.

**Criminal Investigator, GS-1811**

Selective Factor: Ability to conduct computer forensics and analysis involving suspected criminal acts within the contexts of criminal investigations involving highly technical computer networks, infrastructure, and software programs requiring exceptional levels of cyber security expertise and knowledge.

Sample Specialized Experience:
- Planning and coordination computer crime investigations with other Federal criminal investigators and worldwide law enforcement agencies such as: the Defense Criminal Investigative Service (DCIS), Federal Bureau of Investigation (FBI), Air Force Office of Special Investigations (AFOSI), Naval Criminal
Investigative Service (NCIS), Allied and other foreign country's national police forces, and other Federal, state, and local police agencies;

- Conducting timely collection, preservation, and protection of extremely sensitive and often perishable evidence;
- Planning and conducting large scale raids/searches, and often dangerous, undercover or surveillance operations;
- Leading and conducting intricate or delicate criminal/computer investigations involving senior public officials or multinational corporations having continuing political or media interest;
- Conducting Crime Prevention Surveys and vulnerability assessments in support of information assurance, ensuring the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information technology/cyber-security programs, policies, procedures, and tools;
- Planning for the accomplishment of all cyber-security functions for assigned area, to assure efficient and expeditious accomplishment;
- Providing direction, as required, on system vulnerability assessments, using specialized Automated Data Processing software;
- Advising and briefing superiors on sensitive policy issues and problems, making recommendations in critical areas, and initiating authoritative professional action, as necessary, to eliminate cyber threat and system vulnerability.

Information Technology Specialist (Policy and Planning), GS-2210

Selective Factor: Ability to conduct military operations/contingency planning and policy development for cyberspace operations in order to operate network and information systems as well as to protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:

- Developing, implementing, modifying, and maintaining long and short range IT planning;
- Developing and recommending organizational-wide IT goals, objectives, policies and priorities;
- Integrating organizational input and documentation in the development of organizational IT Plans and revises and maintains such plans as required including involvement with both long and short range aspects of such plans;
- Providing advice and guidance to managers in meeting strategic goals;
- Providing oversight, direction, guidance and advisory services to all organizational division and separate office managers concerning unplanned and/or non-programmed needs included in strategic plans;
- Ensuring all organizational information management initiatives are created and maintained in an approved IT tracking system;
- Providing comprehensive management advisory services and liaison to all organizational levels pertinent to emerging and future advances in information technology applicable locally;
- Developing organizational policies and broad-based plans to protect the integrity and confidentiality of automated systems, networks, data, and automation resources/functions.

Information Technology Specialist (Systems Administration)/(System Analysis), GS-2210

Selective Factor: Ability to design, configure, operate and administer information and network systems in order to operate network and information systems as well as to protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:

- Conducting system administration studies, recommending necessary IT action pertinent to all aspects of network support;
- Planning and scheduling the installation of new or modified hardware, operating systems and software applications;
- Coordinating and reviewing the testing of vendor-provided software;
• Accomplishing continuing review of hardware and software ensuring that it is responsive to user needs;
• Managing accounts, network rights and access to systems and equipment;
• Managing system resources, the installation and integration of systems fixes and workarounds, updates, and enhancements including performance, capacity, availability, serviceability and recoverability;
• Identifying and recommending considerations for use in local IT standard operating procedures;
• Maintaining systems configuration, identifying and resolving IT equipment/software interfaces and interoperability problems;
• Analyzes planned logic and workflow through the computer and related equipment and develops planned approaches or revisions necessary;
• Identifies and coordinates the development of sample test data needed to simulate all possible conditions designed into the planned automated systems.

Information Technology Specialist (Enterprise Architecture)/(Operating System), GS-2210

Selective Factor: Ability to analyze, plan, design, implement, document, assess, and/or manage cyberspace enterprise structural framework to align IT strategy, plans, and systems in order to operate network and information systems as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:
• Reviewing, validating, and performing comparison analysis, cyber risk assessment, and mitigation on various architecture information requirements, developing draft recommendations on ways to improve system security;
• Evaluating current and proposed systems to determine shortcomings or enhancements required to attain full utilization of system capabilities;
• Defining, developing, integrating and presenting business processes, system requirements, systems functions and business practices to senior leaders for incorporation into organizational IT systems and/or modules.
• Coordinating functional mapping and rationalization efforts;
• Integrating unique requirements, individual process improvement efforts, and evaluation;
• Providing sound recommendations to higher echelons on system or process integration proposals.

Information Technology Specialist (Applications Software), GS-2210

Selective Factor: Ability to design, document, develop, modify, test, install, implement, and/or support new or existing applications software in order to operate network and information systems as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:
• Interpreting and utilizing communications computer programming concepts, techniques, and directives relative to information system;
• Applying advanced programming techniques in the development of new applications software;
• Providing guidance on varied computer/telecommunications systems and equipment in the study, design, and development of state-of-the-art software;
• Developing, reviewing and updating system level documentation including technical, functional and subsystem descriptions;
• Presenting technical briefings to project personnel and prepares task status schedules and reports;
• Conducting technical training for team members and personnel of other divisions of the agency.

Information Technology Specialist (Network), GS-2210

Revised 14 May 2010
Selective Factor: Ability to plan, analyze, design, develop, test, configure, install, implement, integrate, maintain, and/or manage networked systems used for the transmission of information in order to operate network and information systems as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:
- Creating, designing, and/or maintaining IP networks and the ability to configure and troubleshoot routers, switches, firewalls, VPN concentrators, IDS/IPS and other IP devices;
- Isolate the nature of network system failures and equipment problems, and initiate corrective measures and possible resolutions;
- Monitor and audit the LAN, evaluating the operational problems and recommending improvement or enhancements to the Network AD operations;
- Preparing testing and implementation plans, establishing test criteria and data to ensure all program modules and outputs for assigned project are tested for completeness and accuracy;
- Preparing network system logs and other records of network operations including documentation of network equipment operations problems, network system malfunctions, network system status and resolves trouble calls on network issues and documents any corrective actions.

Information Technology Specialist (Data Management), GS-2210

Selective Factor: Ability to plan, develop, implement, and administer IT systems for the acquisition, storage, and retrieval of data in order to operate network and information systems as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:
- Developing and maintaining local procedures of networks, system operations, and product assembly and installation; and
- Preparing program user documentation, instructions, and installation procedures;
- Planning, coordinating and accomplishing broad and complex studies to identify and determine technical data requirements and specifications and the database applications, equipment and facilities necessary to develop, modify and apply data management systems;
- Designing, developing, implementing, monitoring, maintaining and enhancing the necessary system(s) to support cyber security needs;
- Coordinating studies and plans with IT managers as well as administrative and technical personnel at all levels;
- Recommending conversion to automated systems/databases where none currently exist or Recommending modifications or workarounds to facilitate the enhance cyber security within the overall provisions of standardized systems;
- Developing work plans, program logic, special instructions and detailed flow charts covering processes covered and data management needs.

Information Technology Specialist (Internet), GS-2210

Selective Factor: Ability to conduct technical planning, design, development, testing, implementation, and/or management of Internet, intranet, and extranet activities, including systems/applications development and technical management of websites in order to operate network and information systems as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:
- Planning, designing, developing, testing, implementing, and managing internet and intranet activities (as well as, other computer based visual media), including systems/applications development, installation, configuration, implementation, and technical management of web sites;
- Applying technical knowledge of internet systems, services, and technologies;
• Researching state-of-the-art web site development tools and technology, implementing such tools and technology on organizational web page development systems;
• Determining overall technical design and structure of internet services, monitoring functionality, security, and integrity of internet services;
• Troubleshooting and resolving technical problems with design and delivery of internet services, evaluating new internet services and technologies.

Information Technology Specialist (Customer Support), GS-2210

Selective Factor: Ability to plan and deliver customer support services, including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements, in order to operate network and information systems as well as protect, detect, and mitigate IT and cyberspace vulnerabilities.

Sample Specialized Experience:
• Diagnosing and resolving problems in response to customer reported incidents;
• Receiving and diagnosing problems reported by users of the network, Internet and other assigned systems;
• Determining appropriate corrective action and providing resolution to customer;
• Consulting with customer to determine if problem is best resolved by the establishment of new hardware, software, or network requirement;
• Researching, evaluating, and providing feedback on problematic trends and patterns in customer support requirements;
• Analyzing server performance, network utilization, and trouble reports to devise and provide quality support to organizational personnel;
• Advising and recommending to senior management customer assistance capabilities required for current and new information technology systems;
• Determining systemic problems and consulting with higher level personnel to implement corrective action.