



**DELIVERY ORDER DR-33-06-317**

**TASK ORDER (73)**

**Personal Identity Verification Card Issuance System  
Certification and Accreditation (C&A) Support**

**1.0 OBJECTIVE**

The Contractor shall support the Nuclear Regulatory Commission (NRC) in certifying and accrediting its Personal Identity Verification Card Issuance (PCI) System. The PCI System is comprised of the following systems:

- ACS – Authentication and Credentialing Services - This is a General Support System with a sensitivity of Confidentiality (H), Integrity (H), and Availability (M).
- ITI – Information Technology Infrastructure System - This is a General Support System with a sensitivity of Confidentiality (H), Integrity (H), and Availability (H).
- BASS – Business Applications Support System - This is a General Support System with a sensitivity of Confidentiality (H), Integrity (H), and Availability (H).
- ACCESS – Automated Access Control and Computer Enhanced Security System - This is a Major Application with a sensitivity of Confidentiality (H), Integrity (H), and Availability (M).
- IPSS – Integrated Personnel Security Systems - This is a Major Application with a sensitivity of Confidentiality (M), Integrity (M), and Availability (M).

The objective of this task order is to develop the security deliverables to support a National Institute of Standards and Technology (NIST) Special Publications (SP) 800-79 certification for the PCI System used at the NRC.

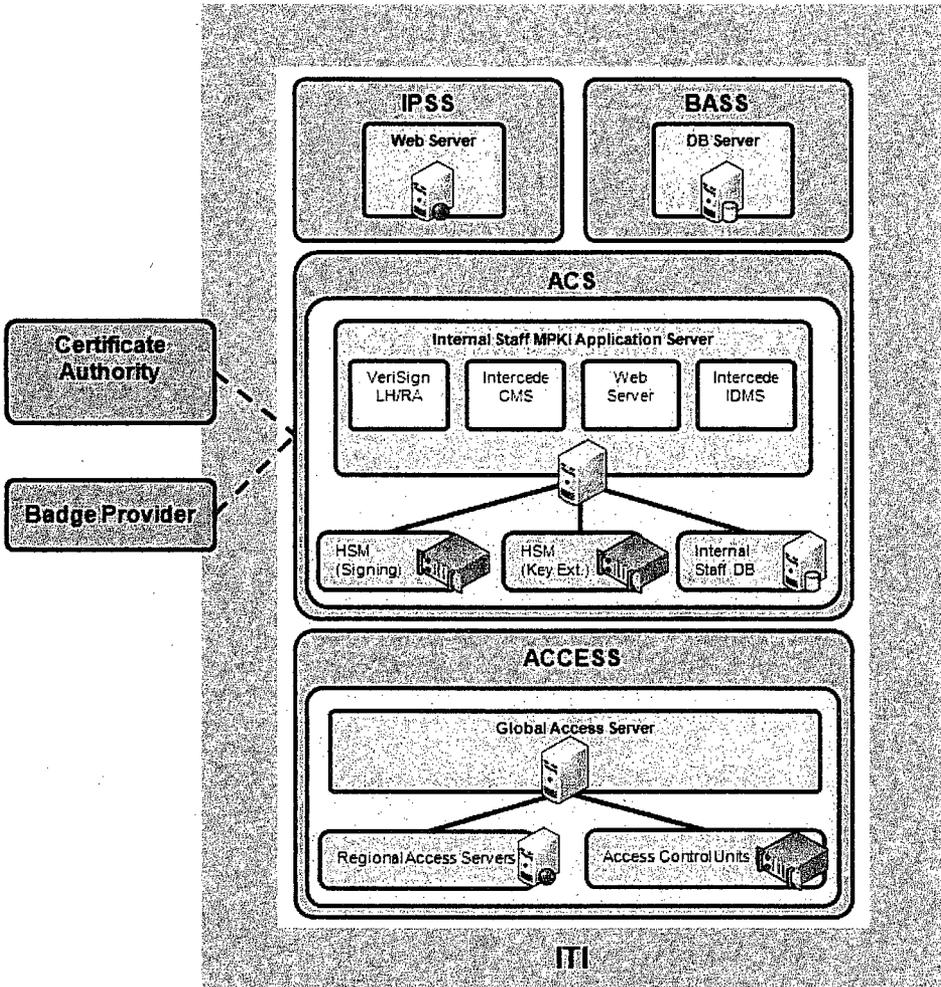
**2.0 BACKGROUND**

The following summarizes the systems that the Contractor shall be working with:

**PCI System**

The NRC developed and implemented the PCI System in order to enhance security at the agency, increase efficiency, reduce identity fraud, and protect personal privacy. The system will allow the NRC to be in compliance with Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard (FIPS) 201-1. To meet these requirements, the PCI System is comprised of General Support Systems and Major Applications, which can issue and maintain FIPS-201-1 compliant badges.

The PCI System leverages services provided by the IPSS, ACS, and ACCESS to meet security requirements identified in HSPD-12 and FIPS 201-1. These three systems support the strong verification of personal identity and access, provisioning and maintenance of Personal Identity Verification (PIV) badges containing users' credentials, and physical access controls to control access to facilities with issued PIV badges. The PCI System relies on BASS and ITI to provide database and network infrastructure services respectively. The PCI System will issue HSPD-12 compliant badges to agency employees and contractors.



**3.0 PERIOD OF PERFORMANCE**

The period of performance for this task order is September 10, 2009 through September 09, 2010.

**4.0 FUNDING**

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$157,747.43** (includes **\$5,000** for NTE travel).
- (b) The amount presently obligated with respect to this task order is **\$80,000.00**. The Contractor shall not be obligated to incur costs above this ceiling/obligated amount unless and until the Contracting Officer shall increase the amount obligated. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified is done so at the Contractor's sole risk.

**5.0 SCOPE OF WORK**

The Contractor must ensure the PCI System has been implemented according to federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The Contractor shall identify any

operational risks found that may affect the system’s ability to perform its mission and protect its data (stored and transmitted). The Contractor shall perform the following:

| <b>Tasks</b>  | <b>NRC PCI System</b>  | <b>Owned By</b>  |
|---|--|--|
| Sub Task 2 - Operations Plan  | Shall develop the PCI System’s Operation Plan.                   | System Owner   |
| Sub Task 3 - Assessment Report  | Shall develop the PCI Assessment Report.                         | Certification Agent - Contractor performing the review<br><br>System Owner will only receive a PDF version of the Assessment Report. |
| Sub Task 4 - Plan of Action and Milestone (POA&M) Report.   | Shall develop the draft PCI Plan of Action and Milestone Report. | System Owner   |
| Sub Task 5 - Certification Package <ul style="list-style-type: none"> <li>• Operations Plan</li> <li>• Assessment Report</li> <li>• POA&amp;M Report</li> <li>• Authority to Operate (ATO) Letters</li> </ul> | Shall put together the Certification Package for the PCI System. | System Owner   |

The Contractor shall provide the necessary security support staff to support the tasks specified in this Statement of Work.

**6.0 SCHEDULE**

The Contractor shall provide security documentation and reports for each system consistent with the NRC-approved integrated project plan (Subtask 1). The Contractor shall ensure that the Certification Package for the PCI System is delivered by 11/13/2009.

**7.0 TASKS**

The Contractor shall support the NRC’s efforts to certify and accredit the PCI System according to SOW Enclosure 6 Section B “Schedule of Supplies or Services and Prices”.

**Subtask 1: Integrated Security Activity Project Plan**

The Contractor shall develop and implement a project plan to ensure the completion of the tasks identified in this SOW occur as expected. The Contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling. These deliverables shall be developed at the individual project level (i.e., each system for which a certification and accreditation effort will be undertaken) and aggregate to the program level. The Project Plan shall incorporate all tasks and projects such that the individual projects roll up into an Integrated Security project schedule encompassing all NRC security related activities, services, and deliverables. The Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels. The Project Plan shall include:

- **Level 5 Work Breakdown Structure (WBS)**

The WBS shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks or groups of tasks (work packages) with decisive outputs and specific measurable entry and exit criteria. Each work package shall have a short duration, or can be divided into a series of milestones whose status can be objectively measured. Each work package shall be assigned a start and finish date, a budget value, and can be integrated with higher-level schedules.

- **Schedule and Budget**

The schedule and budget shall identify what resources are needed, identify how much effort is required, and when each of the tasks specified in the WBS can be completed. The Contractor shall allocate a portion of the budget for each work package that comprises the WBS, and ensure that the WBS adequately defines all work necessary to meet the requirements for the project.

## **Subtask 2: Operations Plan**

The PCI operations plan contains the PCI's policies, procedures, and processes for all the major PCI functional areas. The operations plan provides a complete picture of the structure, management, and operations of the PCI to the Certification Agent and the Designated Approving Authorities (DAA). One of the most significant pieces of information contained within the operations plan is the list of PCI controls, how they were implemented, and who is responsible for their management. This description makes it a simple process for the Certification Agent to quickly ascertain how they were implemented and by whom.

If certain functions described in the operations plan are outsourced, the PCI's operation plan can reference or "point to" the external service provider's operation plan and related documentation, such as support agreements and any contracts. In this manner, the Certification Agent has access to the information regarding the external service provider's operations without requiring the PCI to duplicate any documentation.

The operations plan shall be developed using the template found in NIST 800-79 Appendix D. This template contains the following sections:

1. Background  
<Provide a brief background on HSPD-12, FIPS 201-1 and Personal Identity Verification (PIV), as well as how the organization has planned to meet the Directive. >
2. Purpose and Scope  
<Describe the purpose and scope of the operations plan.>
3. Applicable Laws, Directives, Policies, Regulations and Standards  
<Identify all Laws, Directives, Policies, Regulations and Standards that govern PIV Card issuance at the Organization.>
4. PCI Roles and Responsibilities  
<Identify the accreditation-related roles and responsibilities of all key personnel within the PCI.>
5. Assignment of Roles  
<Document how the various roles that have been identified in the section above are appointed. These can be either specific individuals or positions within the organization. Provide contact information for all the roles assigned.>
6. PCI Description  
<Provide a description of the organization's PCI. Details such as structure and geographic dispersion should be included.>
7. PCI Facility Details

<Identify all the PCI Facilities that are included within the PCI that are part of the accreditation boundary. Provide details such as the location, PIV Card functions performed (e.g. enrollment and/or registration) at the facility and the approximate number of PIV Cards supported at each facility. >

## 8. PCI Management

<This section discusses various management aspects of the PCI. >

- Coordination and Interaction - <Describe management interactions within the PCI, both at an organization level, and between the organization and the facility(s). >
- Staffing - <Describe the procedures employed to make sure that adequate staff is available for performing PIV Card related functions. >
- Training - <Describe the procedures employed to ensure that the staff is properly trained to perform their respective duties. >
- Procurement - <Describe the mechanism typically used for procuring products/services related to the organization's HSPD-12 implementation. >
- Outsourcing - <Describe the PIV Card functions being outsourced at the PCI (if applicable). >

## 9. Policies and Procedures

<Describe in this section the various policies and procedures that apply for (i) sponsorship, (ii) Enrollment and Identity proofing, (iii) Adjudication, (iv) card production, (v) card activation and issuance and (vi) maintenance. Also discuss the procedures for temporary badges, as well as for non-PIV badges employed by the organization.>

- a. Sponsorship
- b. Enrollment/Identity Proofing
- c. Adjudication
- d. Card Production
- e. Card Activation/Issuance
- f. Maintenance
  - Card Termination
  - Card Renewal
  - Card Re-issuance
- g. Temporary/Non-PIV Badges

## 10. PCI Information System Description

<Provide a description of the technical aspects of the organization's PIV system, including system architecture, network connectivity, connections to external system and information shared both internally and externally, the Public Key Infrastructure (PKI) provider as well as the information system accreditation status.>

- Architecture
- Interconnections and Information Sharing
- Information System Inventory
- PKI
- SP 800-37 C&A Information

## 11. Card Personalization and Production

<Describe the organization's PIV Card graphical layout(s), as well the optional data containers being used. Provide details if there are any PIV Card expiration date requirements levied by the organization. Also describe the mechanisms in place for securing both pre-personalized and personalized PIV Card stock >

- PIV Card Graphical Topology
- PIV Card Electronic Data Elements
- Expiration Date Requirements
- Card Inventory Management

#### 12. Card Reporting Requirement

<Describe how the organization collects information from its facilities relating to the number of PIV Cards issued, background investigations completed etc, as required by Office of Management and Budget (OMB). Also provide detail on how the organization consolidates this information and provides its report to OMB on the status of their HSPD-12 implementation.>

#### 13. PCI Controls

<This section documents the PCI Controls and provides the following information for each: (i) PCI control identifier and description, (ii) control owner, (iii) whether the control is organization-specific or facility-specific and (iv) description of how the PCI control has been implemented by the organization>

- PCI Control Identifier and Description
- PCI Control Owner
- Organization/Facility Specific
- How the PCI control is implemented

#### **Appendix A - Memoranda of Appointment**

<Attached copies of signed memoranda-of-appointment that record the various roles that have been assigned and the personnel fulfilling these roles that have accepted the position and its associated responsibilities.>

#### **Appendix B - Privacy Requirements**

<Attached copies of the privacy-related information as identified below.>

- a. Privacy Policy
- b. Privacy Impact Assessment
- c. System of Record Notice
- d. Privacy Act Statement/Notice
- e. Rules of Conduct
- f. Privacy Processes
  - Requests to review personal information
  - Requests to amend personal information
  - Appeal procedures
  - Complaint procedures

#### **Appendix C – Service Level Agreements, Memoranda of Understanding (MOU)**

<Attached copies of any service level agreements and memoranda of understanding executed between the organization and any external service provider that has been contracted to provide certain PIV related functions.>

### **Subtask 3: Assessment Report**

The Assessment report contains the results of the assessment in a format that facilitates reviewing by the DAAs. The DAAs must evaluate the information in the Assessment report in order to make a sound, credible decision regarding the residual risk of authorizing the operations of the PCI System.

An Assessment report shall follow the template found in Appendix E of NIST SP 800-79. The report is organized by Accreditation Focus Area. For each PCI control, it must be documented as to which entity is responsible for the implementation of that control (the organization or an external service provider) and if the PCI control is at the organizational or facility level.

The assessment result associated with each PCI control shall be one of the following:

- Satisfied
- Partially Satisfied
- Not Satisfied
- Not Applicable

After carrying out an assessment procedure, the Certification Agent records his/her conclusion in one of two ways: MET, NOT MET. Using the list of conclusions pertaining to assessment procedures associated with a PCI control, the assessment result (which is one of the 4 outcomes listed above) is arrived at as follows:

- If the conclusion from all assessment procedures is MET, then the assessment result for the PCI control is "Satisfied"
- If some of the conclusions are NOT MET, then the assessment result for the PCI control is marked as either "Partially Satisfied" or "Not Satisfied", depending on whether or not any of the underlying tasks in the assessment procedures are critical (i.e., they represent the only way to meet the PCI control's objective).
- In drawing a conclusion after carrying out an assessment procedure, the Certification Agent must consider the potential subjective and objective aspects of the assessment methods used (e.g., interviews, document reviews, observations, and tests) for that assessment procedure. Deficiencies that result in "Partially Satisfied" or "Not Satisfied" must be reported by the Certification Agent. The Certification Agent must also outline the potential adverse impacts if the PCI control is deployed with the identified deficiencies.

The assessment report provides the means for recording the assessment result for each PCI control. The assessment results for all PCI controls are aggregated to generate the assessment report for a PCI accreditation focus area. The set of PCI Accreditation Focus Area Reports is aggregated to generate a PCI accreditation topic report. Finally, the group of PCI Accreditation Topic Reports is used to generate the overall PCI Assessment Report and an accompanying Executive Summary (intended for Senior Management).

### **Subtask 4: POA&M Report**

The PCI POA&M Report shall utilize NRC standard template and shall address the Corrective Action Plan (CAP) requirements found in NIST SP 800-79. The PCI POA&M Report describes actions that must be taken by the Organization Identity Management Official (OIMO) to correct deficiencies identified in the Assessment phase.

The PCI POA&M Report identifies:

**GS35F0229K DR-33-06-317-T073**

- (i) the tasks to be accomplished
- (ii) the resources required to accomplish the tasks
- (iii) scheduled completion dates for the tasks
- (iv) the person designated as responsible for completing each of the tasks

**Subtask 5: Certification Package**

The Contractor is responsible for the assembly and compilation of the accreditation submission package with inputs from the OIMO. The accreditation submission package shall contain:

- (i) the final assessment report;
- (ii) the PCI POA&M Report;
- (iii) the revised PCI operations plan;
- (iv) NIST SP 800-37 accreditation letters for all information systems within the PCI System.

The contents of the accreditation submission package must be protected in accordance with organization policy.

**8.0 TRAVEL**

Travel is optional and shall not exceed \$5,000.00.

**9.0 MEETINGS**

At the request of the NRC, the Contractor's technical representative shall attend bi-monthly status meetings at NRC Headquarters to discuss work being performed under this task order. The task's Project Manager and any additional staff specified by the NRC Project Officer working on the task must attend. Additional Staff members will receive 48 hours notice that their attendance is required.