|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Personnel Security Plan**  **Document Version: 1.0.0**  **{DATE}** |
| Prepared by: {ORGANIZATION}  **DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.**  **OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO: {ORGANIZATION}** |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Changes Made / Section(s) |
| {DATE} | 1.0.0 | {ORGANIZATION} | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Amplifying Guidance**

1. DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)" [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/520002_2014.pdf)
2. DoD Regulation 5200.02-R, "Personnel Security Program (PSP)", as amended [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf)

**Table of Contents**

[**1.0** **OVERVIEW** 1](#_Toc450028940)

[**2.0** **PERSONNEL SECURITY POLICIES AND PROCEDURES** 1](#_Toc450028941)

[**3.0** **POSITION RISK DESIGNATION** 1](#_Toc450028942)

[**4.0** **PERSONNEL SCREENING** 2](#_Toc450028943)

[**5.0** **PERSONNEL TERMINATION** 2](#_Toc450028944)

[**6.0** **PERSONNEL TRANSFER** 2](#_Toc450028945)

[**7.0** **ACCESS AGREEMENTS** 3](#_Toc450028946)

[**8.0** **THIRD-PARTY PERSONNEL SECURITY** 3](#_Toc450028947)

[**9.0** **PERSONNEL SANCTIONS** 4](#_Toc450028948)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 5](#_Toc450028949)

[**ENCLOSURE 1 – POSITION DESIGNATION** 24](#_Toc450028950)

[**ENCLOSURE 2 – PERSONNEL TERMINATION CHECKLIST** 26](#_Toc450028951)

[**ENCLOSURE 3 – PERSONNEL TRANSFER CHECKLIST** 28](#_Toc450028952)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc447181008)

# **OVERVIEW**

The purpose of the [DoD Personnel Security Program](http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf) is to establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of defense, and granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to information are clearly consistent with the interests of national security.

This Personnel Security Plan ensures that {ACRONYM} follows and implements the [DoD Personnel Security Program](http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf).

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix A, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| [PS-1](#PS1) | Personnel Security Policy and Procedures | P1 | PS-1 | PS-1 | PS-1 |
| [PS-2](#PS2) | Position Risk Designation | P1 | PS-2 | PS-2 | PS-2 |
| [PS-3](#PS3) | Personnel Screening | P1 | PS-3 | PS-3 | PS-3 |
| [PS-4](#PS4) | Personnel Termination | P1 | PS-4 | PS-4 | PS-4 (2) |
| [PS-5](#PS5) | Personnel Transfer | P2 | PS-5 | PS-5 | PS-5 |
| [PS-6](#PS6) | Access Agreements | P3 | PS-6 | PS-6 | PS-6 |
| [PS-7](#PS7) | Third-Party Personnel Security | P1 | PS-7 | PS-7 | PS-7 |
| [PS-8](#PS8) | Personnel Sanctions | P3 | PS-8 | PS-8 | PS-8 |

Table 1 - SP-800-53v4 Compliance Matrix

# **2.0 PERSONNEL SECURITY POLICIES AND PROCEDURES**

DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R. DoD has defined the roles as organizational personnel with access control responsibilities. DoD disseminates DoD 5200.2-R via the DoD Issuance site: http://www.dtic.mil/whs/directives/corres/pub1.html to meet the DoD requirements for personnel security policy and procedures.

# **3.0 POSITION RISK DESIGNATION**

Proper position designation is the foundation of an effective and consistent suitability and personnel security program. In order to ensure a systematic, dependable, and uniform way of making position designations, OPM provides the [Position Designation Automated Tool (PDT)](https://www.opm.gov/investigations/background-investigations/position-designation-tool/#url=Automated-Tool) for those individuals within agencies charged with position designation responsibilities.

The Position Designation System assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service from misconduct of an incumbent of a position. This establishes the risk level of that position. This assessment also determines if a position’s duties and responsibilities present the potential for position incumbents to bring about a material adverse effect on the national security, and the degree of that potential effect, which establishes the sensitivity level of a position. The results of this assessment determine what level of investigation should be conducted for a position.

[Enclosure 1](#Enclosure1) of this document lists the Position Designations and record of review, which must be performed annually.

# **4.0 PERSONNEL SCREENING**

Personnel screening ensures all government and contract personnel meet the appropriate ADP/IT level designation requirements IAW DoD 5200.2-R prior to authorizing access to the {ACRONYM}.

Is the {ACRONYM} Access List contained in the Access Control Artifact?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

Has the appropriate Position Designation clearance level been granted for personnel on the {ACRONYM} Access List?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

Rescreening ensures that personnel assigned to the {ACRONYM} are periodically verified to ensure they still meet Position Designation requirements. The conditions required for rescreening follow established Defense Security Service (DSS) processes.

# **5.0 PERSONNEL TERMINATION**

The purpose of this section is to define post-employment requirements for the protection of {ACRONYM} information. The process defined in this section is in addition to {ACRONYM} policies, such as Security Clearance termination. Reasons for termination vary and are facilitated through the Human Resources and Legal Departments.

The checklist, found in [Enclosure 2](#Enclosure2) of this document, will be utilized to ensure that terminated personnel no longer have access to {ACRONYM} information and all property is properly returned.

Have any personnel assigned to {ACRONYM} been terminated within the last year?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes, is the Personnel Termination Checklist ([Enclosure 2](#Enclosure2)) on file?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **6.0 PERSONNEL TRANSFER**

The purpose of this section is to document and implement a process to modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. It is assumed that the person being transferred is still in good employment standing and requires continued access to DoD IT systems.

The checklist, found in [Enclosure 3](#Enclosure3) of this document, will be utilized to ensure that transferred personnel no longer have access to {ACRONYM} information and all property is properly returned. Access and authorizations for newly assigned systems will follow the SAAR process.

Have any personnel assigned to {ACRONYM} been transferred within the last year?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes, is the Personnel Transfer Checklist ([Enclosure 3](#Enclosure3)) on file?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **7.0 ACCESS AGREEMENTS**

{ACRONYM} utilizes DD Form 2875 (System Access Authorization Agreement (SAAR)) as the methodology to request and grant access to {ACRONYM}. In addition to the SAAR, if a user has administrative rights a Privileged Access Agreement (PAA) must also be signed.

{ACRONYM} requires that individuals re-sign SAARs to maintain access to {ACRONYM} when access agreements have been updated or when there is a change to the user's level of access.

In the event a person is terminated or transferred, the Checklist contained in [Enclosure 2](#Enclosure2) or [Enclosure 3](#Enclosure3) will be used to document the action.

Do all personnel identified in the Access Control List have a valid SAAR on file?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **8.0 THIRD-PARTY PERSONNEL SECURITY**

All third parties providing support to {ACRONYM} must meet DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 and any {ACRONYM} policies for personnel security.

Does {ACRONYM} employ Third Parties for support?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes, does the contract require compliance with DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 and any {ACRONYM} policies for personnel security?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

In addition to any existing contract requirements, third-party providers are required to notify at a minimum, the ISSO and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately. [Enclosure 2](#Enclosure2) and [Enclosure 3](#Enclosure3) of this document contain checklists that must be completed for all third-party providers in the event of personnel termination or transfer.

The Contracting Officer’s Technical Representative (COTR) is responsible for monitoring third-party provider compliance with personnel security requirements.

# **9.0 PERSONNEL SANCTIONS**

In the event personnel fail to comply with established information security policies and procedures for {ACRONYM}, formal sanctions will be employed.

The ISSO will be immediately notified when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Formal Sanctions are part of the general personnel policies and procedures for the {ACRONYM}. The process addresses the following:

* Informal corrective actions.
* Formal disciplinary actions.
* Severe disciplinary actions.
* Removal of system access.
* Possible criminal and/or civil penalties.

NOTE: Any person who improperly discloses classified or sensitive information is subject to criminal and civil penalties and sanctions.

Have Formal Sanctions been performed for any {ACRONYM} personnel?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes, was the ISSO immediately notified?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **APPENDIX A – DETAILED COMPLIANCE MATRIX**

The following table provides traceability between this document and the Assessment Procedures contained within NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations".

| Control Number | Assessment Number | CCI | Confidentiality | Integrity | Availability | Assessment Procedures | Reference |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PS-1 | PS-1 (a) | CCI-003017 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the roles as organizational personnel with access control responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (a) | CCI-003018 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the roles as organizational personnel with access control responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (a) (1) | CCI-001504 | High Moderate Low | High Moderate Low | High Moderate Low | DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (a) (1) | CCI-001505 | High Moderate Low | High Moderate Low | High Moderate Low | DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (a) (2) | CCI-001509 | High Moderate Low | High Moderate Low | High Moderate Low | DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (a) (2) | CCI-001510 | High Moderate Low | High Moderate Low | High Moderate Low | DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (b) (1) | CCI-001507 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (b) (1) | CCI-001506 | High Moderate Low | High Moderate Low | High Moderate Low | DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (b) (2) | CCI-001508 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-1 | PS-1 (b) (2) | CCI-001511 | High Moderate Low | High Moderate Low | High Moderate Low | DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-2 | PS-2 (a) | CCI-001512 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documentation of the ADP/IT level designations. | [Section 3](#_3.0_POSITION_RISK)  [Enclosure 1](#Enclosure1) |
| PS-2 | PS-2 (b) | CCI-001513 | High Moderate Low | High Moderate Low | High Moderate Low | DoD 5200.2-R meets the DoD requirements for establishing screening criteria for individuals filling organizational positions.   DoD organizations are automatically compliant with this control as they are covered at the DoD level by DoD 5200.2-R. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-2 | PS-2 (c) | CCI-001514 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment reviews the audit records of the position designation reviews to ensure reviews are done annually.   DoD has defined the frequency as annually. | [Section 3](#_3.0_POSITION_RISK)  [Enclosure 1](#Enclosure1) |
| PS-2 | PS-2 (c) | CCI-001515 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-3 (1) | PS-3 (1) | CCI-001520 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines security clearance data for all individuals using the classified information system and the system account list (AC-2) and compares lists to ensure all personnel accessing the system are cleared and indoctrinated to the highest classification level of the information to which they have access on the system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PS-3 (2) | PS-3 (2) | CCI-001521 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines security clearance data for all individuals using the classified information system and the system account list (AC-2) and compares lists to ensure all personnel accessing the system are formally indoctrinated for all of the relevant types of information to which they have access on the system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PS-3 (3) | PS-3 (3) (a) | CCI-003019 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of access authorizations to ensure individuals accessing an information system processing, storing, or transmitting information requiring special protection have valid access authorizations that are demonstrated by assigned official government duties. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PS-3 (3) | PS-3 (3) (b) | CCI-003020 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process to ensure that individuals accessing an information system processing, storing, or transmitting information requiring special protection satisfy additional personnel screening criteria defined in PS-3 (3), CCI 3021. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PS-3 (3) | PS-3 (3) (b) | CCI-003021 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented additional personnel screening criteria to ensure the organization being inspected/assessed defines additional personnel screening criteria that individuals accessing an information system processing, storing, or transmitting information requiring protection must satisfy.    DoD has determined the additional personnel screening criteria is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PS-3 | PS-3 (a) | CCI-001516 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the information system access list (AC-2) and compares a sampling of authorized users to manning documents (PS-2) to ensure access was granted appropriately IAW ADP/IT level designation requirements within DoD 5200.2-R. | [Section 4](#_4.0_PERSONNEL_SCREENING) |
| PS-3 | PS-3 (b) | CCI-001517 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines audit records of rescreening actions to ensure the system owner is rescreening individuals according to a system owner-defined list of conditions requiring rescreening and, where re-screening is so indicated, based on the system owner-defined frequency of such rescreening. | [Section 4](#_4.0_PERSONNEL_SCREENING) |
| PS-3 | PS-3 (b) | CCI-001518 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documentation of conditions requiring rescreening of individuals for access to the information system.   DoD has determined the list of conditions is not appropriate to define at the Enterprise level. | [Section 4](#_4.0_PERSONNEL_SCREENING) |
| PS-3 | PS-3 (b) | CCI-001519 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documentation defining the required frequency for rescreening individuals for access to the system.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | [Section 4](#_4.0_PERSONNEL_SCREENING) |
| PS-4 (1) | PS-4 (1) (a) | CCI-003027 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the record of notifications of post-employment requirements to ensure the organization being inspected/assessed notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information. | [Section 4](#_4.0_PERSONNEL_SCREENING) |
| PS-4 (1) | PS-4 (1) (b) | CCI-003028 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the personnel security procedures and a sampling of signed acknowledgments of post-employment requirements to ensure the organization being inspected/assessed requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 (2) | PS-4 (2) | CCI-003029 | High | High | High | The organization conducting the inspection/assessment examines the configuration of the automated mechanism and any records of notification sent to ensure the organization being inspected/assessed implements automated mechanisms to notify at a minimum, the ISSO and personnel responsible for revoking credentials upon termination of an individual.   DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 (2) | PS-4 (2) | CCI-003030 | High | High | High | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-4 | PS-4 (a) | CCI-001522 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines organizational security policy and procedures documentation and audit records of account termination actions to ensure account termination actions are conducted immediately and IAW organizational security policy and procedures.   DoD has defined the time period as immediately. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 | PS-4 (a) | CCI-003022 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as immediately. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-4 | PS-4 (b) | CCI-003023 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of records of termination/revocation of any authenticators/credentials to ensure the organization being inspected/assessed terminates/revokes any authenticators/credentials associated with the individual upon termination of individual employment. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 | PS-4 (c ) | CCI-003024 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented information security topics to ensure the organization being inspected/assessed defines information security topics to be discussed while conducting exit interviews.   DoD has determined the information security topics are not appropriate to define at the Enterprise level. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 | PS-4 (c ) | CCI-001523 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documentation of departed personnel and the audit trail of conducted exit interviews to ensure all departed personnel had exit interviews conducted that include a discussion of information security topics defined in PS-4, CCI 3024. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 | PS-4 (d) | CCI-001524 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines appropriate organization security-related organizational information systems-related property documentation/logs and compares to audit trail of all retrieved security-related organizational information systems-related property (AU-2) to ensure all property has been retrieved. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 | PS-4 (e ) | CCI-001525 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment interviews appropriate IT and security personnel to validate the organization has procedures in place which, upon termination of individual's employment, will ensure it retains access to organizational information formerly controlled by the terminated individual. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 | PS-4 (e ) | CCI-001526 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment interviews appropriate IT and security personnel to validate the organization has procedures in place which, upon termination of individual's employment, will ensure it retains access to organizational information systems formerly controlled by the terminated individual. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 | PS-4 (f) | CCI-003016 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines records of termination notification to ensure the organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for revoking credentials immediately or within 24 hours upon termination of individual employment.   DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials.   DoD has defined the time period as immediately or within 24 hours. | [Section 5](#_5.0_PERSONNEL_TERMINATION)  [Enclosure 2](#Enclosure2) |
| PS-4 | PS-4 (f) | CCI-003025 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-4 | PS-4 (f) | CCI-003026 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as immediately or within 24 hours. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-5 | PS-5 (a) | CCI-001527 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure that the organization has confirmed the ongoing operational need for logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization. | [Section 6](#_6.0_PERSONNEL_TRANSFER)  [Enclosure 3](#Enclosure3) |
| PS-5 | PS-5 (b) | CCI-001528 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines appropriate organization security-related organizational physical and logical access documentation/logs and compares to transferred personnel documentation to ensure appropriate logical and physical access have been revoked for previous positions and granted for new positions immediately.    DoD defines the time period as immediately. | [Section 6](#_6.0_PERSONNEL_TRANSFER)  [Enclosure 3](#Enclosure3) |
| PS-5 | PS-5 (b) | CCI-001529 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-5 | PS-5 (b) | CCI-001530 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD defines the time period as immediately. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-5 | PS-5 (c ) | CCI-003031 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of accounts of users recently transferred or reassigned to ensure the organization being inspected/assessed modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. | [Section 6](#_6.0_PERSONNEL_TRANSFER)  [Enclosure 3](#Enclosure3) |
| PS-5 | PS-5 (d) | CCI-003032 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines records of transfer/reassignment notifications to ensure the organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for transferring credentials within 24 hours when individuals are transferred or reassigned to other positions within the organization.   DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.   DoD has defined the time period as within 24 hours. | [Section 6](#_6.0_PERSONNEL_TRANSFER)  [Enclosure 3](#Enclosure3) |
| PS-5 | PS-5 (d) | CCI-003033 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-5 | PS-5 (d) | CCI-003034 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as immediately. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-6 (2) | PS-6 (2) (a) | CCI-001536 | blank | blank | blank | The organization conducting the inspection/assessment obtains a list of organizational individuals with active accounts and validates the existence of signed DD Form 2875 (paper or electronic) associated with individuals requiring access to classified information with special protection. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PS-6 (2) | PS-6 (2) (b) | CCI-001537 | blank | blank | blank | The organization conducting the inspection/assessment reviews access agreements; access authorizations; personnel security criteria; along with other relevant documents or records to ensure the organization has granted authorized access to classified information requiring special protection only to those individuals who have satisfied the associated personnel security criteria. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PS-6 (2) | PS-6 (2) (c) | CCI-001538 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the access roster and requests the signed nondisclosure agreements of a sampling of individuals to validate the organization requires all access to classified information requiring special protection is granted only to individuals who have a signed nondisclosure agreement. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PS-6 (3) | PS-6 (3) (a) | CCI-003038 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the records of notifications of post-employment requirements for protection of organizational information to ensure the organization being inspected/assessed notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information. | [Section 7](#_7.0_ACCESS_AGREEMENTS) |
| PS-6 (3) | PS-6 (3) (b) | CCI-003039 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of signed acknowledgements to ensure the organization being inspected/assessed requires individuals to sign an acknowledgement of legally binding post-employment requirements for protection of organizational information, if applicable, as part of granting initial access to covered information. | [Section 7](#_7.0_ACCESS_AGREEMENTS) |
| PS-6 | PS-6 (a) | CCI-003035 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented access agreements to ensure the organization being inspected/assessed develops and documents access agreements for organizational information systems. | [Section 7](#_7.0_ACCESS_AGREEMENTS) |
| PS-6 | PS-6 (b) | CCI-001532 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail to ensure review/update occurred annually and departed employees no longer have valid access agreements. | [Section 7](#_7.0_ACCESS_AGREEMENTS) |
| PS-6 | PS-6 (b) | CCI-001533 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-6 | PS-6 (c ) (1) | CCI-001531 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains a list of organizational individuals with active accounts and validates the existence of signed DD Form 2875 (paper or electronic) associated with a sampling of individuals selected from the list. | [Section 7](#_7.0_ACCESS_AGREEMENTS) |
| PS-6 | PS-6 (c ) (2) | CCI-003036 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines a sampling of re-signed access agreements to ensure the organization being inspected/assessed requires that individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or when there is a change to the user's level of access.   DoD has defined the frequency as when there is a change to the user's level of access. | [Section 7](#_7.0_ACCESS_AGREEMENTS) |
| PS-6 | PS-6 (c ) (2) | CCI-003037 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as when there is a change to the user's level of access. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-7 | PS-7 (a) | CCI-001539 | High Moderate Low | High Moderate Low |  | DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 meet the DoD personnel security requirements including security roles and responsibilities for third-party providers.   DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-7 | PS-7 (b) | CCI-003040 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires third-party providers to comply with personnel security policies and procedures established by the organization. | [Section 8](#_8.0_THIRD-PARTY_PERSONNEL) |
| PS-7 | PS-7 (c ) | CCI-001540 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the personnel security requirements to ensure the organization being inspected/assessed documents personnel security requirements for third-party providers. | [Section 8](#_8.0_THIRD-PARTY_PERSONNEL) |
| PS-7 | PS-7 (d) | CCI-003041 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires third-party providers to notify at a minimum, the ISSO and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately.    DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.   DoD has defined the time period as immediately. | [Section 8](#_8.0_THIRD-PARTY_PERSONNEL) |
| PS-7 | PS-7 (d) | CCI-003042 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-7 | PS-7 (d) | CCI-003043 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as immediately. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-7 | PS-7 (e ) | CCI-001541 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring activity to ensure the organization being inspected/assessed monitors third-party provider compliance with personnel security requirements. | [Section 8](#_8.0_THIRD-PARTY_PERSONNEL) |
| PS-8 | PS-8 (a) | CCI-001542 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the organizational security policy to ensure it addresses formal procedures for sanctions and interviews security personnel to validate the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. | [Section 9](#_9.0_PERSONNEL_SANCTIONS) |
| PS-8 | PS-8 (b) | CCI-003044 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the records of notifications of employee sanctions to ensure the organization being inspected/assessed notifies at a minimum, the ISSO immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.   DoD has defined the personnel or roles as at a minimum, the ISSO.    DoD has defined the time period as immediately. | [Section 9](#_9.0_PERSONNEL_SANCTIONS) |
| PS-8 | PS-8 (b) | CCI-003046 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as immediately. | Automatically compliant with this CCI because they are covered at the DoD level |
| PS-8 | PS-8 (b) | CCI-003045 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |

# **ENCLOSURE 1 – POSITION DESIGNATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | AUTHORIZED POSITION DESIGNATIONS | | | |
| Position Designation | | **Applicable** | **Investigation/Form** | **Last Reviewed** |
| Low Risk Non-Sensitive NACI | |  | SF-85 | {REVIEW\_DATE} |
| Moderate Risk Non-Sensitive (Public Trust) MBI | |  | SF-85P | {REVIEW\_DATE} |
| High Risk Non-Sensitive (Public Trust) | |  | BI (SF-85P) | {REVIEW\_DATE} |
| Low Risk Non-Critical Sensitive | |  | ANACI or NACLC (SF-86) | {REVIEW\_DATE} |
| Moderate Risk Non-Critical Sensitive | |  | MBI (SF-86) | {REVIEW\_DATE} |
| High Risk Non-Critical Sensitive | |  | SSBI (SF-86) \*Note- access is still Secret even though investigation is an SSBI. | {REVIEW\_DATE} |
| Critical Sensitive (automatic high risk) | |  | SSBI (SF-86) | {REVIEW\_DATE} |
| Special Sensitive (automatic high risk) | |  | SSBI (SF-86) | {REVIEW\_DATE} |

# **ENCLOSURE 2 – PERSONNEL TERMINATION CHECKLIST**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PERSONNEL TERMINATION CHECKLIST | | | | | | |
| PERSON INFORMATION | | | | | | |
| Name: Enter text. | | | | Title: Click or tap here to enter text. | | |
| Organization: Enter text. | | Location: Click or tap here to enter text. | | | | Phone: Click or tap here to enter text. |
| SYSTEM INFORMATION | | | | | | |
| System Name: Enter text. | | | | System Location: Enter text. | | |
| Administrative Access: | Yes | | No | | | |
| Remote Access: | Yes | | No | | | |
| System Classification: | Classified | | | | Unclassified | |
| ACTIONS | | | | | | |
| Credentials Revoked: | Yes | No | | Notes: | | Enter text. |
| Data archived: | Yes | No | | Notes: | | Enter text. |
| CAC returned: | Yes | No | | Notes: | | Enter text. |
| Based Badge returned: | Yes | No | | Notes: | | Enter text. |
| Hardware returned: | Yes | No | | Notes: | | Enter text. |
| SAAR Responsibilities review: | Yes | No | | Notes: | | Enter text. |
| HR Exit Interview: | Yes | No | | Notes: | | Enter text. |
| Notes: Enter text. | | | | | | |
| USER SIGNATURE | | | | | | |
| Signature: | | | | | Date: Enter a date. | |
| VALIDATION | | | | | | |
| Name: Enter text. | | | | | Title: Enter text. | |
| Signature: | | | | | Date: Enter a date. | |

# **ENCLOSURE 3 – PERSONNEL TRANSFER CHECKLIST**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PERSONNEL TRANSFER CHECKLIST | | | | | |
| PERSON INFORMATION | | | | | |
| Name: Enter text. | | | | Title: Click or tap here to enter text. | |
| Organization: Enter text. | | Location: Click or tap here to enter text. | | | Phone: Click or tap here to enter text. |
| SYSTEM INFORMATION | | | | | |
| System Name: Enter text. | | | | System Location: Enter text. | |
| Administrative Access: | Yes | | No | | |
| Remote Access: | Yes | | No | | |
| System Classification: | Classified | | | Unclassified | |
| ACTIONS | | | | | |
| Credentials Revoked: | Yes | No | | Notes: | Enter text. |
| Data archived: | Yes | No | | Notes: | Enter text. |
| CAC returned: | Yes | No | | Notes: | Enter text. |
| Base Badge returned: | Yes | No | | Notes: | Enter text. |
| Hardware returned: | Yes | No | | Notes: | Enter text. |
| SAAR Responsibilities review: | Yes | No | | Notes: | Enter text. |
| Notes: Enter text. | | | | | |
| USER SIGNATURE | | | | | |
| Signature: | | | | Date: Enter a date. | |
| VALIDATION | | | | | |
| Name: Enter text. | | | | Title: Enter text. | |
| Signature: | | | | Date: Enter a date. | |