Approved for release by ODNI on 04/04/2024, FOIA Case # DF-2022-00157

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
INSTRUCTION 94.03
Category 94 - Cyber Security
Office of Primary Responsibility: Chief Operating Officer/ODNI Chief Information Officer
Revision 2

SUBJECT: (U) DESIGNATION OF PRIVILEGED USERS

1. (U) AUTHORITIES: The National Security Act of 1947, as amended; and other applicable provisions of law.

2. (U) REFERENCES: 44 United States Code, *Federal Information Security Management Act (FISMA) of 2014*; Executive Order 13587; Committee on National Security Systems (CNSS) Glossary 4009; ODNI Principal Executive Memorandum (b)(3) *Improving the Management of Privileged Users at the Office of the Director of National Intelligence (ODNI)*, October 21, 2019; Intelligence Community Policy Memorandum 500 (01), *Enhanced Oversight of Privileged Users in the Intelligence Community Information Environment*, June 21, 2019; ODNI Instruction 94.06, *Disabling, Archiving, and Deleting ODNI User Accounts*; ODNI Instruction 94.08, *Cyber Security Events and Incidents*; ODNI Instruction 112.01, *Security Clearances and Access to Classified Information*; ODNI Instruction 117.02, *Counterintelligence and Insider Threat Training Requirements*; and ODNI Instruction 117.05, *ODNI Insider Threat Program*.

3. (U) PURPOSE: This Instruction establishes policy on the minimum requirements for designation as a Privileged User and the management of Privileged Users in the ODNI, including the insider threat and security responsibilities for Privileged Users as administrators of all ODNI information systems. This Instruction replaces ODNI Instruction 94.03, *Designation of Privileged Users, Revision 1*, October 22, 2018.

4. (U) APPLICABILITY: This Instruction applies to ODNI permanent cadre employees; ODNI staff reserve cadre employees (i.e., time-limited); Highly Qualified Experts; federal civilian detailees; military detailees; Intergovernmental Personnel Act detailees; Presidential appointees; and contractors (hereinafter, "ODNI personnel"). Assignees to the ODNI may not serve as a Privileged User on any ODNI information system.

Approved for release by ODNI on 04/04/2024, FOIA Case # DF-2022-00157

5. (U) DEFINITIONS: For the purposes of this Instruction, the terms used hereinafter are defined in the Appendix.

6. (U//~~FOUO~~) POLICY: Privileged Users have important roles in protecting ODNI information and systems due to their broad administrative and technical privileges. Adherence to this policy ensures that ODNI information and systems are afforded the protection required, and that only those individuals required to manage networks, systems, or applications efficiently, and with minimal interruption, are authorized to perform the elevated administrative functions of a Privileged User. (b)(3) [redacted]

A. (U//~~FOUO~~) **Limitation on Number of Privileged Users:** Deputy Directors, Center Directors, and Heads of Independent Offices (hereinafter, "Senior Officials") will limit the number of Privileged Users designated in their components, and will designate only those individuals who are required to administer component networks, systems, and applications, (b)(3) [redacted]

B. (U//~~FOUO~~) **Security Requirements:** Privileged Users on all ODNI Top Secret-Sensitive Compartmented Information (TS-SCI) information systems must be eligible for access to TS-SCI. Privileged Users on ODNI classified systems must adhere to ODNI Instruction 112.01 and ICPM 500 (01), and must have successfully completed a counterintelligence (CI) polygraph and, if required by the system, compartmented access indoctrinations commensurate with the classification level of the system(s) supported. (b)(3) [redacted] All Privileged Users are subject to enhanced monitoring including enrollment in the Continuous Evaluation program. Privileged Users on other government agency systems must adhere to the system owner requirements.

C. (U) **Training requirements:** ODNI personnel requesting Privileged User access must complete the initial (b)(3) [redacted] course prior to requesting Privileged User access. If data transfer is part of the Privileged User's duties, then the (b)(3) [redacted] (b)(3) course is required. Each year thereafter, Privileged Users must complete the (b)(3) [redacted] (b)(3) course.

D. (U) **Insider Threat Requirements:** In the performance of their assigned duties, Privileged Users must understand and support the requirements outlined in ODNI Instructions 117.02 and 117.05 in order to protect information and observe sound security and CI practices.

E. (U) **Requesting a Privileged User Account:** ODNI personnel requesting Privileged User access must submit a request for an account via the (b)(3) [redacted] (b)(3) application and provide all required information and approvals.

F. (U//~~FOUO~~) **Use of Privileged User Account:** Privileged Users will be assigned a Privileged User account in addition to their General User account. The Privileged User account must be used to perform the privileged activities for which it is specifically intended. The General User account will be used to perform all general activities such as reading emails, creating documents, or browsing

Approved for release by ODNI on 04/04/2024, FOIA Case # DF-2022-00157

websites. Instant messaging may be used with either account. Willful violation or misuse of Privileged User access may result in administrative and/or judicial action. Failure of a Privileged User with System Administrator duties to adhere to Section 7.J.(7)(c-e) below may result in administrative and/or judicial action. Using a General User account to perform Privileged User actions is prohibited and may result in administrative and/or judicial action.

G. (U) **Removal of Privileged Users:** When Privileged Users depart or are otherwise relieved of the designation as a Privileged User, it is the responsibility of the Government Program Manager (GPM) or Contract Officer Technical Representative (COTR) to request removal of the Privileged User account within one business day and comply with ODNI Instruction 94.06 via the ODNI CIO-designated enterprise-wide access request application.

H. (U//~~FOUO~~) **Exceptions:** If any requirement in this Instruction cannot be met, contact the ODNI Information System Security Manager (ISSM) for guidance. (b)(3) [redacted]

I. (U//~~FOUO~~) **Incidents:** In accordance with ODNI Instruction 94.08, Privileged Users are obligated to immediately report cases of data loss, compromise, data spillage, or other incidents to the ODNI ISSM.

7. (U) RESPONSIBILITIES:

A. (U) The Chief Operating Officer will provide policy oversight.

B. (U) The ODNI CIO will:

(1) (U) Implement this Instruction; and

(2) (U//~~FOUO~~) In collaboration with the Chief, ODNI CI and Security (b)(3) [redacted] (b)(3) and maintain related documentation.

C. (U) The ODNI CISO will:

(1) (U) Ensure Privileged Users' compliance with this Instruction in coordination with the GPM or COTR;

(2) (U//~~FOUO~~) Maintain a list of all Privileged Users within ODNI; report the list quarterly to the ODNI CIO; and share the list with the ODNI CI and Security Office for cross-coordination;

(3) (U) Report any security and CI related activities to the ODNI CI and Security Office, as outlined in ODNI Instruction 94.08; and

(4) (U) Inform the responsible GPM and COTR when there are concerns involving a contractor.

Approved for release by ODNI on 04/04/2024, FOIA Case # DF-2022-00157

D. (U//~~FOUO~~) The ODNI ISSM will, upon notification of unusual or suspicious activity, conduct an investigation and ensure the activity has been reported in the *ODNI Security and Counterintelligence Online Reporting (SCOR)* database.

E. (U//~~FOUO~~) The Chief, ODNI Continuous Monitoring will, in coordination with the ODNI CI and Security Office, implement security mechanisms for monitoring Privileged Users; (b)(3) [redacted] and upon discovery of inappropriate and/or malicious activity, coordinate with the ODNI ISSM to monitor or disable the account.

F. (U) The Chief, ODNI CI and Security Office will:

(1) (U//~~FOUO~~) Evaluate reports submitted by ODNI personnel regarding insider threat issues involving Privileged Users and, in coordination with the ODNI CIO, take appropriate actions;

(2) (U//~~FOUO~~) Provide guidance and oversight for any ODNI ISSM-referred cases involving Privileged Users where an insider threat matter may be involved; ensure that appropriate response action(s) or referrals are taken; and ensure the timely resolution of each matter; and

(3) (U) Collaborate with the ODNI CIO with regard to (b)(3) [redacted] (b)(3) [redacted]

G. (U) The ODNI Chief Financial Executive/Senior Procurement Executive and the ODNI Contracts Team will ensure all contracts include a requirement for TS-SCI with CI polygraph as needed by the contract/statement of work.

H. (U) Senior Officials, or designees, will:

(1) (U) Annually approve Privileged Users for their component; and

(2) (U) Limit the number of Privileged Users designated in their components, and designate only those individuals who are required to administer component networks, systems, and applications, especially (b)(3) [redacted] Privileged Users.

I. (U) GPMs or COTRs overseeing Privileged Users will:

(1) (U) Approve the creation, modification, and immediate removal of Privileged User accounts;

(2) (U) Include in their (b)(3) [redacted] Performance Evaluation Report (b)(3) [redacted] an objective requiring they hold all assigned Privileged Users accountable for completing mandatory (initial and annual) Privileged User/cyber security training and meet all minimum requirements stated therein;

(3) (U) Identify required Privileged User roles and Tier assignments for the information system and provide that information in the access request submitted to ODNI CIO;

(4) (U) Confirm need-to-know and verify that the accesses and privileges of each individual

Approved for release by ODNI on 04/04/2024, FOIA Case # DF-2022-00157

are commensurate with the individual's job functions, level of responsibility, and required span of control;

(5) (U) Minimize the number of Privileged Users, especially (b)(3) level;

(6) (U) Perform quarterly reviews of Privileged Users on their managed systems and report to the ODNI CISO through the quarterly data call; and

(7) (U) Upon receipt of a determination that a Privileged User has violated the terms of privileged access, confirm deactivation of Privileged User accounts.

J. (U) Privileged Users will:

(1) (U) Strictly adhere to all standards, directives, instructions, regulations, established security controls, and User Agreements;

(2) (U) Observe sound security and CI practices consistent with security indoctrination, security education and training, and guidance provided by the ODNI ISSM and the ODNI CI and Security Office;

(3) (U) Only use Privileged User accounts to access and perform authorized tasks and functions, and use General User accounts for non-privileged actions/functions;

(4) (U) Include (b)(3) an objective for completing all mandatory (initial and annual) Privileged User/cyber security training and meet all minimum requirements stated therein;

(5) (U) Annually revalidate the continued requirement for access, utilizing the Privileged User workflow/tracking tool and approval process;

(6) (U) Notify the GPM, COTR, and ODNI ISSM when requiring a change of accesses, or when Privileged User access is no longer required due to a change in role and/or duties; and

(7) (U) Privileged Users assigned System Administrator duties will:

(a) (U) Coordinate with GPMs to maintain the currency of all access control lists, and to implement procedures to ensure individuals are immediately removed from access control lists when they no longer require access;

(b) (U) Ensure access permissions are the minimum required by a group or individual to carry out assigned tasks;

(c) (U) Not grant individuals access to directories, subdirectories, shared drives, roots, etc., regardless of the user's position or other privileges, unless authorized by data stewards or mission managers;

(d) (U) Protect the root account by refraining from its use whenever possible and keeping the number of Privileged Users to a minimum; and

Approved for release by ODNI on 04/04/2024, FOIA Case # DF-2022-00157

(e) (U) Not grant Privileged User access to General Users.

8. (U) EFFECTIVE DATE: This Instruction is effective upon signature.

(b)(6) [redacted]

Lora A. Shiao
Chief Operating Officer

8/26/2021
Date

(U) Appendix: Definitions

Approved for release by ODNI on 04/04/2024, FOIA Case # DF-2022-00157

(U) APPENDIX

(U) Definitions

A. (U) **Compromise:** Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. *(CNSSI No. 4009)*

B. (U//~~FOUO~~) **Data Transfer:** Privileged Users can transfer data across classification security boundaries (e.g., from a highly classified domain to a lower classified or unclassified domain) which introduces an enterprise risk worthy of additional attention. Therefore, any user possessing such a role, such as a Data Transfer Officer or Data Transfer Agent (DTO/DTA), is also considered a Privileged User. (b)(3) [redacted] Of note, DTO/DTA personnel may or may not be system administrators.

C. (U) **Data Loss:** The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. *(CNSSI No. 4009)*

D. (U) **Data Spillage:** A security incident that results in the transfer of classified information onto an information system not authorized to store or process that information. *(CNSSI No. 4009)*

E. (U) **General Users:** Individuals who are authorized to use a non-privileged account to perform functions such as reading email, creating documents, or browsing.

F. (U) **Privileged Users:** Individuals who are authorized, and therefore trusted, to perform privileged functions on a network, system, or application. Most often this includes, but is not limited to, individuals who have been granted elevated accesses and rights to ODNI networks, hardware, software, information, or sensitive technical spaces beyond those of General Users or who have the ability to influence others who interact with ODNI information systems, such as Application Managers or Information System Security Managers (ISSMs). Privileged Users are designated (b)(3) [redacted]

G. (U) **Risk-in-position** addresses the risk related to the functions performed and sensitive accesses allocated to an individual. *(ICPM 500 (01))*

H. (U) **Risk-in-data** addresses risk related to the overall volume and sensitivity of data, and access controls in place on the networks to which a user has physical or virtual access. *(ICPM 500 (01))*

I. (U) **Risk-in-person** addresses the risk that an individual either has malicious intent or may develop it in the future. *(ICPM 500 (01))*

J. (U) **Root User:** An individual who has all rights or permissions for a system or application.

Approved for release by ODNI on 04/04/2024, FOIA Case # DF-2022-00157

(b)(3)

[redacted]