Defense Manpower Data Center

Personnel Security & Assurance

Defense Central Index of Investigations (DCII) PKI Frequently Asked Questions (FAQs)

Document Version 1.0

August 23, 2016

Prepared by

DCII Support

This document is current as of January 05, 2015. The following set of responses to FAQs is provided in order to answer common questions regarding the Defense Central Index of Investigations (DCII) PKI logon procedures.

Table of Contents

Section 1: General Questions

1. What are the regulations associated with the DCII PK-enable deployment and why did DMDC remove User ID/Password logon?

a. *For DoD or other Federal Agencies:* Joint Task Force-Global Networking Operations (JFT-GNO) Tasking Order 07-15, Public Key Infrastructure (PKI) implementation, Phase 2 mandates widespread DoD PKI implementation for DoD information systems (including web-servers). Public Key (PK) enabling is further supported by DoD Directive 8500.01E, Information Assurance (IA), and DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling.

2. What should I use to log into DCII and when did the logon methods change?

a. Users need three items to access DCII as of **March 31, 2014**:
   1. An Active DCII account (account management policies have not changed).
   2. An Approved Active PKI Certificate on either a smartcard or USB token (both are considered hardware).
   3. Hardware and Software needed to read the PKI Certificate.
      i. DCII users will need a smartcard reader (hardware) and middleware (software) used to read the PKI certificate on the smartcard credential.
      ii. USB Tokens will only require middleware to be installed to use the PKI certificate.

3. How will DMDC communicate upcoming deployments, releases, modifications, and information regarding DCII?

a. Users can find information on DCII by going to the DCII Welcome Screen within the DCII application as well as the DMDC Personnel Security Assurance (PSA) DCII web pages for alerts, notices, and user guide resources at https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=DCII.

4. How do I get a DCII account?

a. See the DMDC PSA DCII web page Access Request documentation to find out how to get a DCII account. Make sure you have properly completed the Personnel Security System Access Request (PSSAR). To find out what the 'Most Common PSSAR Reject Reasons' are, please review the 'Account Request Instructions' document.

5. What is an active DCII account?

a. An active DCII account is one that has been logged into within the past 30 days. An inactive DCII account is one that has not been logged into within the past 45 days. Your DCII account will be deleted if you do not log into DCII over the course of 45 days per DoD Regulations (APP6240).
b. The 20-minute inactivity timeout rule will still apply.

6. What if I am using my boss, friend or co-worker's User ID/password or PKI credential to log onto the DCII system?

a. It is a violation of DoD Regulations and the PKI providers' User Agreements to share a User ID and password or allow an individual to access another's DCII account or logon credential in any manner or form. Only the authorized account holder is permitted to access/use his/her DCII account; combined or agency user accounts are not recognized or permitted. If you are not using your own account that you requested via submission of an authorized Personnel Security System Access Request (PSSAR) form, STOP USAGE IMMEDIATELY.

   When you enter the DCII system and select 'AGREE', you are agreeing to comply with all DCII administrative policies, including termination of DCII access if terms of use are violated.

7. Will DCII accounts be handled differently (e.g., Personnel Security System Access Request (PSSAR), unlocking of accounts, account management) now that DCII uses a smartcards?

a. DMDC is not changing how accounts are managed at this time. DMDC is only changing login methods for DCII accounts. Please see FAQ #2 in this document for further information. A DCII user will still need to qualify, submit a PSSAR, and be approved to receive a DCII account.
b. A user will have to provide their User ID and a password in order to self-register their PKI certificates.

8. Is a user ID and temporary password required prior to logging in with a PIV?

a. Yes, you must have an active user ID and password prior to accessing DCII as these are utilized on the self-registration page, where your DCII account and PKI credential are correlated.
b. You will only be required to input your User ID and temporary password when registering a new certificate (e.g., when replacing an expired certificate).

9. Will I have to register my hardware PKI each time I log in?

a. No, not if you have only **one** PKI credential. DCII will only present the self-registration page to users whose non-CAC certificates are not already stored in DCII.
b. When your PKI certificate expires and/or are renewed, users will be required to re-register the new certs on the DCII system. Certificate lifecycles can be from 1 to 3 years depending upon what was purchased from the PKI provider.

10. If I log in with a CAC (PIV, or other) card, will I be required to change my password?

a. No, you will not be required to change your password; however, you may be prompted to re-enter your PKI PIN after a period of time. This allows the application to re-authenticate the user.

Section 2: CAC Card, Smart Card and Public Key (PK) Enabling Questions

11. What is a CAC?

a. The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees, state employees of the National Guard, and eligible contractor personnel.

   The CAC is used as a general identification card as well as for authentication to enable access to DoD computers, networks, and certain DoD facilities.

12. What is a Smartcard?

a. A smartcard, chip card, or integrated circuit card (ICC), is any pocket-sized card with embedded integrated circuits. Smartcards may also provide strong security authentication for single sign-on (SSO) within large organizations.

13. What is a smartcard reader?

a. A card reader is a data input device that reads data from a card-shaped storage medium.

14. Who qualifies for a CAC?

a. Eligible populations include Active Duty service members, DoD civilian employees, and DoD contractors who are under DoD contract *and* sponsored by a DoD Service or Agency (DoD Manual (DoDM) 1000.13, Volume 1). Not all DoD personnel are eligible for CACs. DoD Contractors may obtain CACs if their government sponsor deems it necessary and they fulfill one of the three requirements:
   1. Be an active duty or reserve service member, or a DOD civilian
   2. Work on site at a military or government installation
   3. Be a DoD contractor who works on Government Furnished Equipment

b. To find out more information:
   1. On the CAC, you can visit http://www.cac.mil/.
   2. To obtain the DoDM 1000.13, you can visit http://www.dtic.mil/whs/directives/corres/pdf/100013_vol1.pdf.

15. How do I login to DCII with my DoD approved PKI credential (CAC, PIV, or other)?

a. First Time PKI DCII Access Procedures:
   1. Obtain an active DCII account and an active PKI Certificate on a smartcard (CAC, PIV card, ECA PKI Certificate on a smartcard/token, or other approved DoD PKI on a smartcard/token).
   2. Obtain a smartcard reader, smartcard reader driver, and smartcard middleware (if necessary).
      Note: Installation of smartcard readers and smartcard middleware is the responsibility of the Department/Agency that controls the workstation configuration.
      i. Plug the smartcard reader into the Personal Computer (PC).

ii. Install the smartcard reader driver on the PC.
   a. This should either come bundled with the smartcard reader or the PKI provider should include instructions to locate the website where the driver can be downloaded.
   b. If necessary, install smartcard middleware on the PC.

3. Insert the smartcard into the smartcard reader and logon to DCII by selecting "*CAC/PIV Log in"*.
4. If you are logging on with a DoD approved hardware certificate, you will be taken to a self-registration screen.
   i. This screen will ask for your User ID and password, input this information.
   ii. Your PKI credential will now be correlated with your DCII account.

16. I have inserted my PIV and clicked the 'CAC/PIV Log In' button and now I see a Self-Registration screen. What should I do on this screen?

a. DCII will display a new Self Registration screen to allow users to associate (or register) their non-CAC to their active DCII user ID and password. Enter your DCII user ID and password and click the "**Register**" button, then you will be taken into your DCII account.
b. DCII will display a new Self Registration screen if your non-CAC is different from what was previous registered, or you have multiple non-CACs, or a combination of CAC and non-CAC (common amongst users supporting multiple contracts). The Self Registration screen allows users to associate their non-CAC to their active DCII user ID and password. Enter your DCII user ID and password and click the "**Register**" button, then you will be taken into your DCII account. You will be prompted to re-register your non-CAC each time you switch between certificates.
c. The Agency Administrator will not be required to update or add smartcard numbers to his or her DCII user's account. Each user will be required to register his or her own certificate with his or her valid DCII User ID/password the first time he or she logs on. This will link the certificate on the smartcard to his or her active DCII account.

17. What if I don't qualify for a CAC?

a. The use of other DoD approved PKI certificates (e.g., PIV cards, ECA PKI cards, or other DoD approved PKI cards) for DCII access will be authorized. See question 18 'c' and 'd' for more information on other DoD approved PKI certificates.

18. What Identity Credentials contain DoD approved PKI certificates?

a. *CAC Cards:* The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees, state employees of the National Guard, and eligible contractor personnel. For more information on CAC, please visit the following web sites:
   - CAC web site at http://www.cac.mil/.
   - On the DoDM 1000.13, you can visit http://www.dtic.mil/whs/directives/corres/pdf/100013_vol1.pdf.
b. *PIV Cards:* Personal Identity Verification (PIV) Cards are required to be issued to all US

Federal employees and contractors under HSPD-12[1] (as well as FIPS 201[2]). Each Federal Agency is responsible for issuing PIV cards to qualifying employees and contractors. Please use your internal procedures such as contacting your Security, IT or Human Resource office to get additional information about determining qualifications for a PIV from your Federal Agency. Your Agency will explain the process for obtaining a PIV card as it varies from Agency to Agency.

- Section 4 of this document lists the Agencies who distribute PIVs.

c. *ECA Credentials:* This is designed to provide contractors a venue to procure DoD approved certificates. Only PKI certificates that have completed Joint Interoperability Test Command testing and received DoD approval for use on DoD systems are authorized for DCII access – do not assume a corporate smartcard qualifies. These need to be at a Medium Token Assurance or Medium Hardware Assurance certificate level. For more information, please visit the following web site:
   - DISA's ECA PKI at http://iase.disa.mil/pki/eca/.

d. *PIV-Interoperable (PIV-I) Credentials:* Non-Federally issued PKI certificates issuers that have completed Joint Interoperability Test Command testing and received DoD approval for use on DoD systems are also authorized for DCII access. For more information, please visit the following web site:
   - Complete list of DoD approved external PKI providers are available at: http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html http://iase.disa.mil/pki-pke/interoperability/index.html
   - See question 25 for further information regarding "other" DoD approved credential providers.

19. Can I access DCII if I have other types of DoD approved PKI certificates?

a. Yes. DMDC has authorized the use of DoD approved PKI certificates other than CACs for DCII as long as they meet the specifications outlined in these FAQs and the 'DoD Approved PKI Providers' document. Question 25 (below) also covers the entities that offer these credentials for sale.

20. Smaller agencies may not have an extensive IT infrastructure. Whom can they call to assist with the certificates and setting up the hardware?

a. The PKI providers have Call Centers that are able to assist various users, including those with no technical background. The PKI provider's Call Centers are able to answer all questions and walk their customers through their processes. All issues with software/hardware should be directed to the PKI providers Helpdesk. If you continue to receive errors, please contact the DMDC Contact Center.

b. The DMDC Contact Center can field calls regarding browser configurations for the DCII PKI Enabling project.

[1] Homeland Security Presidential Directive-12 (HSPD-12) stipulates that personnel requiring regular access for more than 120-days to a Federally-controlled information system or facility shall be issued a PIV Card [1] FIPS 201-2 "Personal Identity Verification of Federal Employees and Contractors"

[2] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

21. How do I get a PKI certificate if I don't qualify for a CAC or my Agency doesn't issue PIVs?

a. If you do not qualify for either a CAC or PIV, coordinate with your agency to obtain a FIPS 140-2 compliant **Medium Token Assurance Certificate on a smartcard or USB Token** or a **Medium Hardware Assurance Certificate on a smartcard** from one of the three DoD ECA currently approved vendors listed below or go to http://iase.disa.mil/pki/eca/ for more information.

IdenTrust, Inc.
Web Site: http://www.identrust.com/certificates/eca/index.html
Email: ECAsales@IdenTrust.com
Phone: 866.299.3335

Operational Research Consultants, Inc.
Web Site: http://www.eca.orc.com/
Email: ecahelp@orc.com
Phone: 800.816.5548

b. Alternately, multiple Non-Federal Issuers (NFI) have been approved for PKI/cryptographic usage within DoD they include all of the Category II listed providers at the following website: http://iase.disa.mil/pki-pke/interoperability/index.html.

c. A list of DoD approved PKI Providers can be found by clicking on this link.

22. Are there any questions I need to ask the ECA vendor when I first call them?

a. Be sure to ask "Do you provide the PKI Medium Token or Medium Hardware certificates on FIPS 140 compliant devices?"
b. "What are the timelines associated with your credential issuance?"
c. "What is your PIN/Password reset policy?"

23. Can USB Tokens be used on DoD Government Furnished Equipment?

a. Yes, FIPS 140-2 USB tokens can be used on DoD Government Furnished Equipment. While there is a DoD Policy prohibiting USB Memory Drives, it does not prohibit using the USB interface to connect a smartcard reader or a FIPS 140-2 validated USB token.

24. What do I do when the PKI vendor offers me a thumb drive instead of a smartcard?

a. The PKI certificate needs to be generated directly on the FIPS 140 compliant device. FIPS 140 compliant Medium Token Assurance USB Tokens are acceptable. Contact your IT department to ensure all internal policies and procedures of your organization will be followed prior to purchasing any PKI related equipment.

25. What hardware will I need to logon to DCII using a smartcard?

a. *A Smartcard Reader* – GSA HSPD-12 Approved Products List is the source for identifying which smartcard readers are authorized for use with the approved PKIs.
b. Please refer to the FIPS 201 Approved Products List for smartcard readers, referred to as "Transparent Readers," located at: http://www.idmanagement.gov/approved-products-list. Simply click Category on the top row to alphabetically sort the list of products. Then scroll down to the list of "Transparent Reader" for the complete listing.

26. What hardware will I need to logon to DCII using a USB Token?

a. Additional hardware will not be required as long as the computer has a USB interface that is available. Additional middleware will be required.

27. What software will I need to logon to DCII using a smartcard/USB Token?

a. *Step One*: Please see your agency's IT staff to ensure your Department/Agency has existing smartcard middleware. Many Departments/Agencies already have existing smartcard middleware within their infrastructure. If your Department/Agency does not have existing smartcard middleware, then go to Step Two.
b. *Step Two*: If your Department/Agency does not have existing smartcard middleware they will need to obtain it. There are over a dozen authorized PIV Middleware products, ranging from DoD's widely used ActivClient to Gemalto's SafesITe FIPS201 Client API. Many approved PKI vendors have the option of bundle deals that include the necessary hardware and software. GSA HSPD-12 Approved Products List is the source for identifying which smartcard middleware is authorized for use with approved PKIs.

Please refer to the FIPS 201 Approved Products List for the smartcard middleware, referred to as 'PIV Middleware' located at: http://www.idmanagement.gov/approved-products-list. Simply click Category on the top row to alphabetically sort the list of products. Then scroll down to the list of "PIV Middleware" for the complete listing.

PKI providers may direct/provide their consumers to specific smartcard readers and/or middleware that work best with their product.

28. If I have a CAC do I need to purchase an additional certificate?

a. No, you will not need to purchase an additional certificate. The CAC serves as verification of identity for an individual; however, you must still have an active DCII account to logon to the application. A CAC with ANY affiliation (Military, Civilian, Contractor) can be used to logon to DCII independent of affiliation. Anyone that has been issued a valid CAC may use it to logon to DCII.
b. If you have not been issued a CAC for your job functions, you will need to acquire a PKI certificate. See question #15 for information about CAC qualifications.

29. What if I forgot the PIN or Password for my credential?

a) This depends on the specific type of credential you are dealing with:
   a. For a DoD CAC, you have 3 attempts to enter a correct PIN, if you fail the 3rd attempt your credential will be locked; in order to unlock you will need to visit a DEERS/RAPIDS station to unlock and subsequently use it.
   b. For a Federal PIV, a similar procedure will be necessary as with the CAC. Check with your local PKI Issuance Office regarding procedures for the Federal PIV cards.
   c. For ECA and other DoD approved PKI credentials this process can vary from issuer to issuer.
      i. Note: some issuers do not conduct a PIN/Password reset and will require the purchase of a separate credential, please be forewarned and ask what the vendor's SOP is prior to purchase.

Section 3: Technical Questions (when attempting to log on with CAC (PIV or other)

Please refer the JPAS PKI Technical Guide to answer your technical questions. This document contains a good deal of information to assist in the resolution of potential issues.

Section 4: Defining Terms for PK-Logon

30. What is PKI?

a. Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA. The term trusted third party (TTP) may also be used for certificate authority (CA). The term PKI is sometimes erroneously used to denote public key algorithms, which do not require the use of a CA.

b. Another explanation of PKI (public key infrastructure) states that it enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

c. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)

d. A public key infrastructure consists of:

1. A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key.
2. A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor.
3. One or more directories where the certificates (with their public keys) are held.
4. A certificate management system.

31. What is FIPS 140-2?

a. FIPS, or Federal Information Processing Standard, 140-2 is a Government computer security standard for accrediting cryptographic modules. The National Institute of Standards and Technology (NIST) issued the FIPS 140 series to coordinate the requirements and standards for cryptography modules that include both hardware and software components.

32. What is FIPS 201?

a. FIPS 201 (Federal Information Processing Standards Publication 201) is a United States federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors. In response to HSPD-12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201 was developed to satisfy the technical requirements of HSPD 12 approved by the Secretary of Commerce, and issued on February 25, 2005. FIPS 201 together with NIST SP 800-78 (Cryptographic Algorithms and Key Sizes for PIV) are required for U.S. Federal Agencies but do not apply to US national security systems. The SmartCard Interagency Advisory Board has indicated that to comply with FIPS 201 PIV II US government agencies should use smart card technology.

b. Though not an official DoD source, for more information you can also visit http://en.wikipedia.org/wiki/FIPS_201.

33. What is middleware?

a. Software that provides a link between separate software applications. Middleware is sometimes called plumbing because it connects two applications and passes data between them. Middleware allows data contained in one database to be accessed through another. This definition would fit enterprise application integration and data integration software. ObjectWeb defines middleware as: "The software layer that lies between the operating system and applications on each side of a distributed computing system in a network.

b. Though not an official DoD source, for more information you can also visit http://en.wikipedia.org/wiki/Middleware.

34. What is HSPD-12?

a. There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.

b. For more information you can also visit http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.

35. How does Public and Private Key Cryptography work?

a. In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA).

The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory). Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital certificate. When I receive it, I can use your public key to decrypt it. Here's a table that restates it:

To do this	Use whose	Kind of key
Send an encrypted message	Use the receiver's	Public key
Send an encrypted signature	Use the sender's	Private key
Decrypt an encrypted message	Use the receiver's	Private key
Decrypt an encrypted signature (and authenticate the sender)	Use the sender's	Public key

36. What is certificate authority?

a. In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many public key infrastructure (PKI) schemes.

b. Though not an official DoD source, for more information you can also visit http://en.wikipedia.org/wiki/Certificate_authority.

37. What is a public key certificate?

a. In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. For provable security this reliance on something external to the system has the consequence that any public key certification scheme has to rely on some special setup assumption, such as the existence of a certificate authority.

b. Though not an official DoD source, for more information you can also visit http://en.wikipedia.org/wiki/Public_key_infrastructure.

Section 5: List of Agencies who distribute PIVs to their employees

Department of State:
http://www.state.gov/documents/organization/121534.pdf

Department of Treasury:
http://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td71-12.aspx

Department of Housing and Urban Development:
http://www.hud.gov/offices/adm/hudclips/forms/files/pivform.pdf

Department of Veterans Affairs:
http://www.va.gov/pivproject/

Department of Labor:
http://www.dol.gov/oasam/doljobs/DOL-PIV-Card-Policy.htm

Department of Interior:
www.doi.gov/hspd12/docs/PIV_Guide_v1_final.doc

Department of Commerce:
http://www.osec.doc.gov/osy/hspd-12/applicants.html

Department of Energy:
http://www.hss.energy.gov/HSPD12/guidance/n2064.pdf

Department of Agriculture:
http://hspd12.usda.gov/index.html

General Services Administration:
http://www.gsa.gov/portal/content/103401

Farm Credit Administration:
http://www.fca.gov/home/policies_notices/personal_identity.html

Farm Credit System Insurance Corporation: http://fcsic.gov/FCSIC%20PIVC.html

Federal Communications Commission: http://www.fcc.gov/hspd-12/

Institute of Museum and Library Services: http://www.imls.gov/about/hspd12.shtm

NASA: http://itcd.hq.nasa.gov/PIV.html

USAccess via GSA: http://www.fedidcard.gov/

This is the list of agencies where the PIV is currently <u>not</u> being distributed:

Department of Justice: Each bureau has its own process

Department of Homeland Security: Each bureau has its own process

Department of Transportation

Department of Education

Department of Health and Human Services

Federal Energy Regulatory Commission

Federal Housing Finance Administration

Federal Labor Relations Authority

Federal Maritime Commission

Federal Reserve Board

International Boundary and Water Commission JMF

National Archives

National Endowment for the Arts

National Transportation Safety Board

National Mediation Board

US Official of Special Counsel

Securities and Exchange Commission Version