Privacy Impact Assessment

Network General Support System

- Version: 3.3
- Date: April 25, 2020
- Prepared for: USDA FSIS OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

Network General Support System (N-GSS)

April 25, 2020

Contact Point

Frances Byrd

Food Safety and Inspection Service (FSIS)

Office of the Administrator (OA)

(202) 708-8758

Reviewing Official

Emmanuel Olufotebi

Privacy Office

United States Department of Agriculture

Revision History*

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
2.1	January 2007		Reformatted and reorganized
2.2	January 2008		Changed title page to match official name
2.3	January 2008		Changed system name within document to match official name
2.4	June 25, 2012	Mark Whitaker	Updated to reflect new department template (from August 2010).
2.5	April 5, 2013	Noel Nazario	Annual Update
2.6	February 19, 2014	Paul Kuscher	Annual Update
2.7	November 20, 2015	Rohan A. Heath	Updated for Authorization to Operate (ATO)
2.8	February 4, 2016	Rohan A. Heath	Updated to new template.
2.9	September 16, 2016	Rohan A. Heath	Annual Update
2.10	September 1, 2017	Rohan A. Heath	Annual Update
2.11	November 15, 2018	Rohan A. Heath	Updated for FY19 Assessment & Authorization (A&A).
2.12	December 7, 2018	Rohan A Heath	Signed by System Owner
2.13	December 13, 2018	Rohan A Heath	Signed by CISO
3.0	December 19, 2018	Rohan A Heath	Updated Authorizing Official
3.1	March 28, 2019	Rohan A. Heath	Updated Privacy POCs. Finalized for CA Binder Meeting

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
3.2	April 10, 2019	Rohan A. Heath	Updated based on feedback from Privacy
3.3	April 25, 2020	Rohan A. Heath	Annual Update

Abstract

This document provides the Privacy Impact Assessment (PIA) for the Food Safety and Inspection Service (FSIS) Network General Support System (N-GSS). The purpose of N-GSS is to provide communication services to FSIS personnel (employees and contractors) and the FSIS applications. The E-Government Act requires agencies to conduct a PIA before developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public. This PIA was developed because N-GSS supports multiple FSIS systems and applications and might disseminate identifiable information collected and processed by them.

Overview

The FSIS Network is a general support system that represents the core components of the FSIS communication infrastructure and is therefore essential to the FSIS mission of ensuring a safe and wholesome food supply for the nation's population. The FSIS Chief Technology Officer is the System Owner for N-GSS. The N-GSS does not store information other than information technology data relating to the administration of network devices, and, as required, the names of system administrators. However, it does provide communications support for other FSIS systems that do store and process information. Network administration data is maintained on the devices that comprise the network infrastructure (routers, switches, intrusion detection system (IDS)/intrusion prevention system (IPS), etc.) and dedicated workstations that provide device management functions.

Every business unit within FSIS relies upon the N-GSS to access enterprise applications, the Headquarters in DC, District Offices (DO), Field Offices (FO), Laboratories, remote sites and establishment offices. The key infrastructure components of the Network GSS consists of agency-owned firewalls, routers, switches, Voice over Internet Protocol (VoIP) telephony, Virtual Private Network (VPN), and wireless network and their related network equipment.

N-GSS facilitates data flow, but does not process any information of its own. N-GSS is primarily housed at the USDA Headquarters in Washington, D.C., and core locations in Kansas City, MO, Saint Louis, MO, Fort Collins, CO, and Beltsville, MD. The N-GSS includes a number of interconnected remote sites that include district offices, Laboratories, the Financial Processing Center (FPC) in Urbandale, IA, the Human Resources Division (HRD) in Minneapolis, MN, the Policy Development Division (PDD) (formerly Technical Services Center in Omaha, NE), the Humane Animal Tracking Service (HATS) Plant, and the Service Depot located in Columbia, MD, (currently supported by General Dynamics IT (GDIT)).

The FSIS primary backbone consists of the FSIS Universal Telecommunications Network (UTN), which is connected to USDA UTN and provides access to the Internet for all USDA agencies. The USDA UTN keeps each Agency's data logically separated. The FSIS UTN relies on three access points (also known as the OCIO backbone) to connect to the USDA UTN and the Internet. They are:

- the FSIS Beltsville Stack, located in Beltsville, MD
- the FSIS Ft. Collins Stack, located in Fort Collins, CO
- the FSIS Headquarters Stack, located in Washington, DC.

Some traffic comes into the FSIS UTN Headquarters Stack directly from the Internet and not via the USDA UTN. Such traffic comes in through secure VPNs that are protected using the Advanced Encryption Standard (AES). The categories of traffic that enter the FSIS UTN this way are:

- Individual user client machines (remote VPN)
- Point-to-Point VPN.

Other remote locations needing to access the FSIS UTN use a variety of different communication technologies.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The N-GSS uses the first initial and lastname of FSIS personnel (employees and contractors that provide Network operations and maintenance support) to create Network Administrator accounts. The N-GSS does not collect, disseminate, or maintain users PII. The N-GSS relies on the United States Department of Agriculture's (USDA's) Enterprise Directory (EAD) to manage and maintain Network Administrators PII (First and Last Names).

1.2 What are the sources of the information in the system?

USDA's Enterprise Active Directory manages and maintains Network Administrator PII and is the source for creating N-GSS Network Administrator accounts.

The Network Administrators have to obtain administrator accounts to access the network components (e.g., routers and switches). Network Administrator accounts are created based on the first initial and last name of a user (Network Administrator).

Like all users of the FSIS environment (FSIS employees and contractors), Network Administrators must have an active EAD user account. When an individual applies for an EAD account, their First and Last Name are provided as part of the request. Though EAD information is maintained by USDA, the FSIS Network ensures that the information provided to and maintained by USDA's EAD is accurate before permitting a user to establish a network session.

1.3 Why is the information being collected, used, disseminated, or maintained?

The N-GSS does not collect, disseminate, or maintain PII. The N-GSS **uses** the first initial and lastname of FSIS personnel (employees and contractors that provide Network operations and maintenance support) to create Network Administrator accounts.

1.4 How is the information collected?

The N-GSS does not collect, disseminate, or maintain PII. All users of the FSIS environment (FSIS employees and contractors) must have an EAD user account. When an individual applies for an EAD account, their First and Last Names are

provided as part of the request. When a Network Administrator applies for a privileged administrator account, the information is provided in the request.

1.5 How will the information be checked for accuracy?

The employee's First and Last Name are vetted at the time an employee is hired and is maintained in EAD. The Employee Number from EAD is generated at the time the employee's user account is created. If an employee's information is incorrect, they will not be able to access the FSIS Network.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The authorities for USDA to collect, maintain, use and disseminate information through this system are: 5 U.S.C.301 (government organization and employees); Title 5 USC 552a (Records Maintained on Individuals (Privacy Act)); Title 41 CFR 201-6.1 (Federal Information Resources Management Regulation); 44 U.S.C.3101 (Records Management); OMB Circular No. A-108 (Responsibilities for the Maintenance of Records About Individuals by Federal Agencies); OMB Circular No. A-130 (Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals); and Authorization to Operate (ATO), dated 22-07-14,

In addition, USDA is generally authorized to collect information to support its mission under: Title 7, Chapter 55-2205 (7 U.S.C 2204) (which authorizes the Secretary of Agriculture to collect information and employ any sampling or other statistical method deemed appropriate); 21 U.S.C. 679c(a)(1)-(3) (which expressly authorizes the Secretary to give high priority to enhancing the ability of FSIS to conduct its mission); the Federal Meat Inspection Act (FMIA) (21 U.S.C. 601, et seq.), the Poultry Product Inspection Act (PPIA) (21 U.S.C., et seq.), the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, et seq.), and the Humane Methods of Livestock Slaughter Act of 1978 (7 U.S.C. 1901-1906).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The N-GSS does not collect, disseminate, or maintain PII. The N-GSS **uses** the first initial and lastname of FSIS personnel (employees and contractors that provide Network operations and maintenance support) to create Network Administrator accounts and relies on the USDA's EAD to manage Network Administrators' PII.

There are minimal privacy risks as the N-GSS does not collect, disseminate, or maintain PII. N-GSS facilitates data flow but does not process any information of its own, but instead transmits PII as required by applications.

In addition, N-GSS System Administrators and general users access the system using unique, authorized accounts. N-GSS cannot be accessed without an authorized account, an FSIS issued laptop, and an IP address from an FSIS authorized IP address range. There are no anonymous user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

There are firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology and Network Administrators must comply with the Agency's Privileged User Rules of Behavior. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years. Active Directory and N-GSS role-based security are used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory.

When anyone is granted access to the FSIS environment, they are issued a USDA email account and an FSIS user account. In addition, they may have to obtain a USDA e- Authentication account (e.g., to access a specific FSIS application). By having these accounts, the user's network login credentials are checked against authorized system user role membership, and access privileges are restricted accordingly. FSIS system users must pass a Government NACI (National Agency Check with Inquiries) background check prior to having system access. Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

All attempts to login to the FSIS network are logged and the FSI Security Operations Center uses the information to monitor access to the network and track the top 10 users with the most failed attempts. In addition, all Network Administrator activity is logged.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The N-GSS **uses** the first initial and last name of FSIS personnel (employees and contractors that provide Network operations and maintenance support) to create Network Administrator accounts.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The FSIS Security Operations Center (SOC) uses numerous tools to monitor the health of and access to the FSIS Network on continuous real-time (24x7) basis. These tools include, but are not limited to, Riverbed, Solar Winds, Splunk, and Symantec Endpoint Protection. These tools provide information about attempts to logon to the network, failed logon attempts, most popular website, known malicious websites, intrusion detection information, equipment problems, the distribution of anti-virus data, etc.

The FSIS Data Center Operations Branch (DCOB) team (i.e., Network Administrators) utilizes the Cisco Secure ACS View interface and Cisco Works. Via this interface, the DCOB team can run reports to review Network Administrator activity. The Cisco Secure ACS View interface provides numerous canned reports that show log on activity, account creation events, changes to the network devices, etc.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The SOC monitors the health of and activity on the FSIS Network. As part of the monitoring effort, the SOC tools displays names of Web Sites to show the most frequently visited sites. The SOC monitoring tools also display the names of known malicious Web Sites to which FSIS is actively blocking access.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

See Section 1.7 above for a description of the controls that have been put in place for the FSIS Network.

There are minimal privacy risks as the N-GSS does not collect, disseminate, or maintain PII. N-GSS facilitates data flow but does not process any information of its own, but instead transmits PII as required by applications.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The N-GSS does not collect, disseminate, maintain, or retain PII. The N-GSS uses the first initial and lastname of Network Administrators to create user accounts, but relies on the USDA's EAD to manage Network Administrators' PII.

USDA's EAD retains Network Administrators information for as long as the user is active. E-GSS Account Operators receive "Report of Separations" and/or and Footprints ticket notifications on a regular basis for users that have separated from the agency. Thereafter, the user's Active Directory account is immediately deleted. In addition, E-GSS administrators perform routine checks regarding the reported separated staff to ensure their accounts are no longer active.

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). FSIS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or agency that requested the personal records. These accounts are to be kept for five (5) years, or the lifetime of the record, whichever is longer. Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject upon request.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

There are minimal privacy risks as the N-GSS does not collect, disseminate, or maintain PII. N-GSS facilitates data flow but does not process any information of its own, but instead transmits PII as required by applications. The USDA's EAD manages the N-GSS PII, and as long as they are maintained, there is a risk that the information could be exposed to unauthorized individuals. The length of time data is retained does not change the level or type of risk associated with retaining the data. Therefore, the same methods to reduce risk are used throughout the life of the data.

See Section 1.7 above for a description of the controls that have been put in place for the FSIS Network.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The N-GSS does not share information with other organizations. N-GSS does confirm that users attempting to logon to the network have an EAD account (maintained by the USDA).

4.2 How is the information transmitted or disclosed?

PII data is not use for reporting or retrieval purposes.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The Network Administrator First Name and Last Names information is not shared with any internal organizations and it is maintained on access controlled tools, so there is little privacy risk.

The general user EAD account information is not maintained by the N-GSS. The handshake to confirm that someone is using an authorized account is encrypted over an access controlled network, so there is little privacy risk.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information is not shared with organizations external to the USDA.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

N-GSS does not share PII outside of the Department.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Should N-GSS information need to be shared externally, departmental guidelines for providing information to such organizations will be followed. This includes the redacting of PII, unless the information is required under law.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

As long as employee PII data is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee PII is not shared externally. Such information would only be provided if required by law. Standard FSIS or USDA guidelines for protecting the information would be followed.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. Notice is provided to the FSIS employees at time of hiring, in accordance with Directive 8010.12 for all Source System users. Plant vendors are provided notification during business agreement processes. If personal information is obtained from an individual, he or she is provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes. Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII) for all Source System users. Plant vendors are provided notification during business agreement processes.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

In accordance with Directive 8010.12, if personal information is obtained from an individual, they are provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA office.

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2166, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 720-2109 - Fax (202) 690-3023 – E-mail: fsis.foia@fsis.usda.gov.

For more information about how to make a FOIA request, please see:

http://www.fsis.usda.gov/wps/portal/footer/policies-and-links/freedom-of-information-act/foia-requests

7.2 What are the procedures for correcting inaccurate or erroneous information?

The employee would contact Human Resources and follow the standard HR procedures for addressing incorrect employee information. In addition, users can contact the FSIS Service Desk at 1-(800) 473-9135.

If a Network Administrator's name is incorrect in his or her Network Administrator account, the Network Administrator would bring to the attention of N-GSS management to have the information corrected.

7.3 How are individuals notified of the procedures for correcting their information?

The FSIS Human Resources (HR) would contact an individual via email if it believes that the individual's information is incorrect, and provide the individual with the procedures to correct their information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

N/A. Formal redress is provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Corrections to the data are securely maintained in the same manner as the original data; therefore, there is no privacy risk associated with redress available to individuals.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

To gain access to the N-GSS system, a general user must have: 1) an account on the FSIS Active Directory, 2) an FSIS issued laptop, and 3) they must be working from an FSIS authorized IP address. Network Administrators must also have a privileged network account in order to access actual network devices (e.g., routers and switches).

Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

8.2 Will Department contractors have access to the system?

Contractors authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Annual, recurring security trainings practiced and conducted through the Office of the Chief Information Officer. Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect of incomplete data as recorded in the system. Contractors who may be authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. An access agreement describes prohibited activities (such as browsing) by authorized users is monitored, logged, and audited. All users are required to undergo Department-approved computer security awareness training prior to access and must complete computer security training yearly in order to retain access.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, the ATO was granted on April 16, 2019. This is an annual update.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, department, and agency policies and procedures are safeguards implemented to mitigate the risks to any information technology.

The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk is that Network Administrator's (federal employee and contractors) First and Last Names are collected and stored in the N-GSS system.

See Section 1.7 above for a description of the controls that have been put in place for the FSIS Network.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

N-GSS is a General Support System.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes. Both M-10-22 and M-10-23 have been reviewed by the SO and ISSPM.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

N/A - Third party websites are not being used.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

N/A - Third party websites are not being used.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A - Third party websites are not being used.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A - Third party websites are not being used.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A - Third party websites are not being used.

If so, is it done automatically?

N/A - Third party websites are not being used.

If so, is it done on a recurring basis?

N/A - Third party websites are not being used.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A - Third party websites are not being used.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A - Third party websites are not being used.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A - Third party websites are not being used.

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of of all uses of web measurement and customization technology?

N/A.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A - Third party websites are not being used.

Responsible Officials

Frances Byrd
System Owner
1400 Independence Ave., SW
Washington, DC 20250

Marvin Lykes
Chief Information Security Officer
1400 Independence Ave., SW
Washington, DC 20250

Carl Mayes
Chief Information Officer (Acting)
1400 Independence Ave., SW
Washington, DC 20250

Emmanuel Olufotebi
Privacy Office
Room 1142, South Building
Washington, DC 20250

Approval Signatures

Barring any major updates, no signatures are required until the ATO expiration date 4/16/2022.