1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: December 8, 2009

(b) Name of system: AlarmNet

(c) System acronym: AlarmNet

(d) IT Asset Baseline (ITAB) number: 885

(e) System description (Briefly describe scope, purpose, and major functions):

The AlarmNet General Support System (GSS) is a single business function system (Physical Access Control Management). AlarmNet utilizes information collected by the Identity Management System (IDMS) to build access profiles and give individuals access to facilities within the Department of State (DOS) (domestically). This information is required to give access clearances, and provide the Department's Diplomatic Security Uniformed Police Officers (UPO) the information necessary to protect Department assets. AlarmNet supports the Bureau of Diplomatic Security (DS/FSE/DME) mission requirements for providing physical intrusion detection, access control security, and monitoring from central locations, for all domestic Department facilities nationwide on a 24x7 basis. AlarmNet provides the connectivity for the Department's Domestic Access Control and Intrusion Detection System. It is the backbone of the system that permits employee and contractor access into the building.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): Certification & Accreditation

(h) Date of previous PIA (if applicable): April 27, 2009

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

AlarmNet does not collect any PII, but maintains PII collected by the Identity Management System (IDMS). The IDMS collects information from employees and members of the public with access to DoS facilities. IDMS passes the information to the Access Control System residing on AlarmNet. The following information is held in the Access Control System:

- Name
- Social Security Number
- Citizenship
- Security Clearance Level
- Birth Date
- Photograph
- Home Address and Phone Numbers
- A minutia representation of the index finger fingerprints

b. How is the information collected?

AlarmNet receives information from IDMS via a single interface. AlarmNet does NOT collect the information.

c. Why is the information collected and maintained?

The information is passed to AlarmNet to build access profiles to give individuals access to facilities within the Department (Domestically). This information is required to give access clearances and provide the Department's Diplomatic Security Uniformed Police Officers (UPO) the information necessary to protect Department assets. AlarmNet provides the connectivity for the DoS Domestic Access Control and Intrusion Detection system. It is the backbone of the system which permits employee, contractor and members of the public with access into the building.

d. How will the information be checked for accuracy?

Information accuracy is the responsibility of the collecting system (IDMS). An automated mechanism copies the data to AlarmNet. Whenever there is a change to the information in the IDMS, it is immediately and automatically replicated to AlarmNet in order to keep it current.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to AlarmNet, are as follows:

- 5 USC 301; Federal Information
- Executive Order 10405 – Security Requirements for Government Employees
- Executive Order 10865 – Safeguarding Classified Information Within Industry
- Executive Order 12958 – Classified National Security Information
- Executive Order 12968 – Access to Classified Information
- Executive Order 12829 – National Industrial Security Program

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

The information copied to AlarmNet is the minimum required to meet the needs of the Bureau of Diplomatic Security (DS) personnel and functions to perform their mission.

The nature of the PII held along with the inherent function of AlarmNet resulted in a security impact categorization of "High" for AlarmNet. This security impact categorization establishes the specific privacy and security controls required.

Given the impact categorization level, the technical and operational controls in place virtually remove any risks relative to privacy due to system infrastructure. The primary remaining privacy risk is exposure due to the human factor.

There are numerous management, operational, and technical security controls in place to mitigate privacy risk, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

There are two uses: first, to build an automated facility access control profile (for use in the access control systems) that defines an individual's authorized access; and, second, to provide an interface to the information for DoS Diplomatic Security UPO forces to aid in executing their chartered security mission.

b. What types of methods are used to analyze the data? What new information may be produced?

No analysis is conducted on the information contained within AlarmNet. The dual purposes for the information are stated in section 4(a). No new information is produced.

c. If the system uses commercial information, publicly available information, or information from other Federal Agency Databases, explain how it is used.

AlarmNet does not use commercial information, publicly available information, or information from other Federal agency databases.

d. Is the system a contractor used and owned system?

AlarmNet is a Government-owned system which was primarily designed and developed by contractors. All contractors have abided to regulatory guidelines and have signed to follow DS's Rules of Behavior.

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

Appropriate use of AlarmNet is regulated by automated controls in AlarmNet and by the System Rules of Behavior for technical support personnel. Additionally, DoS Diplomatic Security UPOs are bound by information use policies proscribed for Federal Law Enforcement.

Instruction for system use is periodically refreshed and re-issued. AlarmNet does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

5. Retention

a. How long is information retained?

Records relating to persons' access covered by this system are retained in accordance with General Records Schedule 18, Item 17 approved by the National Archives and Records Administration (NARA). The records are disposed in accordance with Department disposal policies unless retained for specific, ongoing security investigations. For maximum security facilities, records of access are maintained for five years and then destroyed. For other facilities, records are maintained for two years and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by NARA. The records are disposed in accordance with Department disposal policies. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

In accordance with HSPD-12, PIV Cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by cross-cut shredding no later than 90 days after deactivation

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

AlarmNet maintains names, social security numbers, citizenship information, security clearance levels, birth dates, photographs, home addresses, phone numbers, and a minutia representation of the index finger fingerprints.

In response to these sensitive elements of PII, AlarmNet follows the records disposition schedule recommended in OMB Memorandum M-06-06 and destroys records upon notification of death or not later than five years after separation or transfer of an employee. Since access to DoS building facilities is critical for the physical security of the Department, PIV Cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by cross-cut shredding no later than 90 days after deactivation.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Information contained within AlarmNet is not shared outside of the DoS Diplomatic Security Bureau. The organizations that have access to the information are; DS/DSS/DO/DFP (Diplomatic Security/Diplomatic Security Services/Domestic

Operations/Domestic Facilities Protection – the end users of AlarmNet) and DS/C/ST/FSE (Diplomatic Security/Countermeasures/Security Technology/Facilities Security Engineering – the builders and technical support division for AlarmNet). There is no sharing of information with other DoS Bureaus.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Authorized users are granted access through a user account and login. Authorized users have roles assigned to them specific to their job function. All users must have access to OpenNet prior to gaining access to AlarmNet.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

It is possible for an employee with authorized access working for the Department of State to use his or her access to this information to retrieve PII on an individual and use this information in an unauthorized manner. In order to mitigate this risk all Department employees are required to undergo computer security and privacy awareness training prior to accessing AlarmNet and must complete refresher training yearly in order to retain access.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

No information is shared outside of the Department's Bureau of Diplomatic Security.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

The information is not shared outside the Department.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Information contained within AlarmNet is not shared externally; therefore, the risk to an individual's privacy is very low.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

STATE-36 Information Access Programs Records

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

AlarmNet does not participate in the collection of information. All information contained within AlarmNet is collected via IDMS. IDMS is responsible for providing notice of the purpose, use, and authority for collection of information submitted as described in the System of Records Notices titled STATE-36.

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

The individual is informed of the Privacy Act statement; whereby, the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also described in the System of Records Notice titled STATE-36.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

AlarmNet does not collect information but is supplied information by IDMS. IDMS does not allow conditional consent because it is not applicable to the official purpose of IDMS.

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

IDMS is responsible for the collection of information. The Privacy Act Statement is available on all forms within IDMS. Furthermore; notification is provided to the Public via SORN State-72 (IDMS).

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

AlarmNet contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. However, all information contained within AlarmNet is a replication of data collected by IDMS. In order to make a modification to information contained within AlarmNet the information will first have to be modified within IDMS. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses. Additionally, such procedures are published and available to users at 22 CFR 171.31.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The Business Owner (DS/FSE/DME) approves and authorizes use of the AlarmNet system. All authorized government users maintain a security clearance level commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to AlarmNet requires a unique user account assigned by Diplomatic Security.

Criteria, procedures, controls, and responsibilities regarding access are all documented. Moreover, the Bureau of Diplomatic Security employees and contractors must follow the System Behavior Rules established by the Department. System accounts are maintained and reviewed on a regular basis. The following DoS policies establish the requirements for access enforcement.

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control
- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo Cyber Security Training which encompasses computer security and privacy awareness, prior to accessing the system, and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system generates audit trails which can be reviewed in the event that misuse of the system is suspected. (An audit trail provides a record of the particular functions a particular user performed, or attempted to perform on an information system.)

11. Technologies

a. What technologies are used in the system that involves privacy risk?

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational, and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the

national vulnerability database (NVD), following and implementing sound Federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risk to any information technology. AlarmNet has been designed to minimize risk to privacy data.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational, and technical controls in place to mitigate these risks. These controls are fully described in the System Security Plan (SSP) for AlarmNet. The following are some of the safeguards in place (this is not an exhaustive list; refer to the SSP for further information):

- The system is a fully cryptographically separate network from all telecommunications providers communications for Wide Area Network components.
- Network communications for AlarmNet are all encrypted by FIPS 140-2 required technologies.
- There is no public access to this system.
- All administrative and end user access is closely controlled through appropriate personnel vetting processes and by system authentication and identification technologies.
- The entire AlarmNet GSS has workstation clients dedicated to the singular purpose of monitoring the facility access control mission. They are not used for any other purpose and thus limits potential "leakage" to any other system or process.
- Each server is configured as proscribed by DoS policies and best business practices (most restrictive controls are used).

12. Security

What is the security certification and accreditation (C&A) status of the system?

AlarmNet was authorized to operate November 30, 2006, via the C&A process. The current authorization is expiring. The C&A process for reaccreditation is in progress and should be was complete November 2009 and received an Authorization to Operate which expires November 2012.