

AlarmNet Privacy Impact Assessment

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: 27 April 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). It supports the DS/FSE/DME mission requirements for providing physical intrusion detection, access control security, and monitoring from central locations, for all domestic Department of State (DoS) facilities nationwide on a 24x7 basis. AlarmNet operates with servers, routers, switches, cryptographic WAN link devices, I-Star panels (connected to entry smart card keypads, motion and other sensors), digital video recorders and workstations.
- (f) Reason for performing PIA:
- New system
 - Significant modification to an existing system
 - To update existing PIA to new format**
- (g) Explanation of modification (if applicable): not applicable
- (h) Date of previous PIA (if applicable): 19 May 2006

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?

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

- Name;

AlarmNet Privacy Impact Assessment

- Social Security Number
- Citizenship;
- Security Clearance Level;
- Birth date;
- Photograph;
- Home Address and Phone numbers; and
- A minutia representation of the index finger fingerprints.

b. What are the sources of the information?

The source of information is the IDMS.

c. How is the information collected?

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

d. 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 provides the Bureau of Diplomatic Security's (DS) uniformed police officers (UPO) the information necessary to protect Department assets.

e. 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 systems to keep it current.

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

- 5 USC 301 Federal Information;
- Executive Order 10450 – 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; and
- Executive Order 12829 – National Industrial Security Program

g. 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 DS personnel and the functions to perform their mission.

The nature of the PII held in AlarmNet along with its inherent function resulted in a security impact categorization of "**High.**" The 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 risk due to system infrastructure. The primary remaining privacy risk is exposure due to the human factor.

AlarmNet Privacy Impact Assessment

To mitigate privacy risks, the systems security controls (including human processes and procedures in place to protect privacy) are subject to rigorous testing, a formal certification and accreditation (C&A) process, and authority to operate is authorized by a senior agency official (SAO). Moreover, controls are reviewed annually and accredited every three years or sooner if there are major changes made to AlarmNet as defined by OMB Circular A-130.

4. Uses of the Information

a. Describe all uses of the information.

There are two uses of AlarmNet: the first is to build an automated facility access control profile (for use in the access control systems) defining individuals' authorized accesses; the second is to provide an interface to the information for DS uniformed police officer (UPO) forces to aid in executing their chartered security mission.

b. What types of methods are used to analyze the data?

There is no "analysis" of the information, it is solely used for the purposes stated above.

c. What new information may be produced?

None.

d. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

None used. The system does not use commercial information, publicly available information, or information from other Federal agency databases.

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

AlarmNet is the property of the Bureau of Diplomatic Security, owned by the Department of State. However, contractors use and maintain the operations of the system within Department facilities.

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

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?

PII is maintained in AlarmNet for a period of three years after the last known use of the access control card (the smartcard) to gain access to Department facilities. This is in accordance with the Department's Records Disposition Schedule, Chapter 11 Section 3.

AlarmNet Privacy Impact Assessment

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

Given the security controls in place and abiding by established retention policies, there is no additional residual risk relative to data retention.

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 is only available within the Bureau of Diplomatic Security. The offices 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 Department 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 access to AlarmNet.

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

Refer to item 4(f) above and item 10 below for all applicable controls.

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?**

There is no sharing for information outside the Bureau of Diplomatic Security.

- b. How is the information shared outside the Department?**

Not applicable.

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

Not applicable.

8. Notice

The system:

- constitutes a system of records covered by the Privacy Act.
 does not constitute a system of records covered by the Privacy Act.

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

AlarmNet Privacy Impact Assessment

Information maintained in AlarmNet is collected via the IDMS. Therefore, the opportunity to provide notice is not given and not applicable to this system.

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

Same as item 8a above.

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?

Same as item 8a above.

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.

Not applicable.

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 receives information from the IDMS. Individuals follow the procedures in State-72, Identity Management System, to amend information they believe to be incorrect. AlarmNet replicates information in IDMS.

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

The notice is reasonable and adequate for this system.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access?

Internal access to AlarmNet is limited to authorized Department staff having a need for access to the system in the performance of their official duties. All authorized U.S. Government users maintain a security clearance level at least 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 the Bureau of 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.

b. What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The system maintains a system log of events as required by the security controls for a "High" impact system. Reference pertinent certification and authorization (C&A) documentation for detailed security controls.

AlarmNet Privacy Impact Assessment

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

Every DoS user must attend a security briefing prior to receiving access to Department networks and getting a badge for facility access. This briefing is sponsored by DS/SI/IS also includes the Privacy Act of 1974. Users must also take a Departmental information system security briefing and quiz prior to receiving access to a Department network.

DS/CTO/SMD/SEC regularly updates the user acknowledgment agreement that all users must prescribe to in order to have access to Department networks. DS/SI/CS also has a Departmental Security Awareness Program in-place.

DS/CTO identifies key personnel within DS/CTO/SMD/OPS and DS/CTO/SMD/SEC who need to attend the Department's mandated Information Assurance training for system administrators. DS/CTO/SMD/OPS and DS/CTO/SMD/SEC are responsible for system and security administration on DS owned servers.

d. 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.

Minimal residual risk is anticipated. As with all systems, there exists minimal risk due to potential human influence conditions. However, all automated and physical protections, as well as the best possible personnel vetting processes and procedures are in place to keep the residual risk level to a minimal.

11. Technologies

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

As with all automation systems, there is some possible risk to privacy data used by AlarmNet. The architecture of the system is such to minimize any possible risk and is fully described in the System Security Plan (SSP) and IT Contingency Plan (ITCP) for AlarmNet. Refer to 11(b) below for a highlight of security safeguards in place.

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

The Security Impact Categorization of AlarmNet is "High," thereby mandating the use of the strictest security controls necessary for an automation system. These controls are in place. They are fully described in the System Security Plan for AlarmNet. As an overview, there are multiple layers of safeguards in place to minimize privacy and other security risks. Following are **some** of the safeguards in place (this list is not exhaustive; refer to the SSP for further information):

- The system is a fully cryptographically separate network from all telecommunications providing 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.

AlarmNet Privacy Impact Assessment

- 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 thereby limiting potential “leakage” to any other system or process.
- Each server is configured as proscribed by Department 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 on November 30, 2006, via the C&A Process. The current authorization will expire on November 30, 2009.