Privacy Impact Assessment
for the

Homeland Security Virtual Assistance Center

November 3, 2008

Contact Point
Donald M. Lumpkins
National Preparedness Directorate
Federal Emergency Management Agency (FEMA)
(202) 786-9754

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) National Preparedness Directorate (NPD) operates the Homeland Security Virtual Assistance Center (HSVAC). HSVAC is an advanced web-based, technical assistance management solution that supports FEMA in the scheduling, coordination, and management of training provided to First Responders, including state and local government entities and organizations. FEMA has conducted this privacy impact assessment (PIA) because HSVAC will use and maintain personally identifiable information (PII) to authenticate user identities of those individuals requesting access to the application.

Introduction

FEMA's National Preparedness Directorate provides funding to enhance the capacity of state and local jurisdictions to prevent, respond to, and recover from incidents of terrorism involving chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons and cyber attacks. NPD achieves its mission by providing grants to state and local jurisdictions. This provides hands-on training through a number of residential training facilities and in-service training at the local level, funding and working with state and local jurisdictions to plan and execute exercises, and providing technical assistance on-site to state and local jurisdictions.

State and local entities are required to provide training for their First Responders so that they are better prepared to react to and counter the incidents listed above. By providing interactive capabilities to manage this training, NPD empowers employees to provide and direct training information and cataloged exercises from an environment that is available throughout the year. One of the primary objectives of the HSVAC application is to enhance the capability of state and local jurisdictions as well as special needs jurisdictions such as port authorities and mass transit agencies to respond to terrorist events and natural disasters. The HSVAC application is designed to assist First Responders in developing, planning, and implementing effective strategies for preparedness with regard to chemical, biological, radiological, nuclear, and explosive (CBRNE) attacks.

Users receive accounts after completing registration through the application itself or from being invited by an existing State Authorization Authority/Urban Area Working group (SAA/UAWG), Preparedness Officer or TA Manager. Application administrators, which include the HSVAC Program Manager, TA Manager, Preparedness Officer, and SAA/UAWG are responsible for approving accounts and for confirming the applicant's status as first responders. Federal level administrators are responsible for verifying the accuracy and identity of Federal users, state users, and state administrators; in turn, approved state administrators are responsible for verifying the accuracy and identity of the local administrators. Local administrators are then charged with approving local users when/if local personnel are required to assist the local administrator. Once accounts have been approved, users may use the application to request training through the website catalog. Typically, training cannot be requested or provided until funds for such training are presented by the state, jurisdiction, or special entity on behalf of the user or user group.

Section 1.0 Information Collected and Maintained

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

1.1 What information is to be collected?

During the user registration process, the HSVAC collects the following information (required information marked with an "*")

Personal Details

- First name*
- Last Name*
- Middle Initial
- Title
- Organization*
- Account Type (Local/State/Urban Area, State Authorization Authority (SAA), Urban Area Working Group (UAWG)) and Area*
- State or Urban Area*

Contact Information – user may provide business or personal contact information

- Email*
- Phone number*
- Fax number
- Street Address*
- City*
- State*
- Zip Code*

Security Verification

- Security Question – User provides an answer to one of the following security questions:
  1. What is your pet's name?
  2. What is your mother's maiden name?
  3. What is your father's middle name?
  4. What is your high school mascot?
  5. Who is your childhood best friend?
- Selected and unique username*
- Password*

1.2 From whom is information collected?

This information is collected from DHS employees, contractors, state personnel, and local first responders that are seeking or have been granted an account on the HSVAC system.

1.3 Why is the information being collected?

This information is collected in order to verify the identity of individuals requesting access to the application and to establish access eligibility. Since information within the application may include data which is considered sensitive and does not lie within the public domain, identities for individuals requesting access must be verified and a valid "need to know" must be established.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The following are technical references in terms of documents that govern the way in which the HSVAC system operates:

Information is collected pursuant to Homeland Security Presidential Directive 8 "National Preparedness" (HSPD-8), Homeland Security Presidential Directive 5 "Management of Domestic Incidents" (HSPD-5), the Homeland Security Act of 2002, Privacy Act of 1974 (5 U.S.C. 552a), EO 13111, Using Technology to Improve Training Technologies for Federal Government Employees and the E-Government Act of 2002 (Section 208).

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

The HSVAC application's main purpose is to act as a tool that assists in the provision and scheduling of training and exercises that broaden the capabilities of First Responders. Because some information regarding this training could be considered sensitive, it is necessary for the system to collect PII about those individuals requesting access to the HSVAC. This information is collected so that it may be used to verify the identity and valid "need to know" for each individual that has requested access or that has been granted access. As a part of this information collection process, several security questions are asked of the individuals registering for application use. These questions are utilized by help desk personnel supporting the application in instances where passwords for approved users need to be changed and the identity of those users must once again be verified.

To mitigate the risks associated with collecting PII, the HSVAC has integrated robust security into its risk management plans and through the Certification and Accreditation processes routinely test the security of HSVAC. In addition, in accordance with the DHS Sensitive Systems Handbook, HSVAC ensures effective security controls and authentication. By enforcing system policies and settings and strong passwords, the HSVAC protects the privacy of data to promote or permit public access to the system and to protect the integrity of the data itself. Further, the HSVAC has implemented best practices, such as auditing, to defend against misuse of the data and to monitor those with access to the information.

Section 2.0 Uses of the System and 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 purpose of the HSVAC application is the scheduling, coordination, and management of training for First Responders. Information provided by an individual during the user registration process is used by HSVAC administrators to confirm the individual's identity and eligibility for access. Federal level administrators are responsible for verifying the accuracy and identity of Federal users, state users, and state administrators; in turn, approved state administrators are responsible for verifying the accuracy and identity of the local administrators. Local administrators are then charged with approving local users when/if local personnel are required to assist the local administrator. The user selected "security questions" and related answers are used to verify a user's identity over the phone when a person contacts a support staff member for assistance and to reset a forgotten password. Any other information collected (i.e. authorized user requests for training assistance) by or used within the application is directly related to training services provided by the system.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "datamining")?

The HSVAC system does not have this functionality.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Federal level administrators are responsible for verifying the accuracy and identity of Federal users, state users, and state administrators; in turn, approved state administrators are responsible for verifying the accuracy and identity of the local administrators. Local administrators are then charged with approving local users when/if local personnel are required to assist the local administrator.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The risks to HSVAC PII were identified through a review and analysis of process flow and controls conducted by HSVAC developers, Information Systems Security Officer (ISSO) personnel, administrative personnel, and the HSVAC System Owner. If PII from the HSVAC is shared with an individual or

component not directly associated with the HSVAC, there is a risk that the information could be improperly handled and/or disclosed to unauthorized individuals**.** Access controls in place are accredited by the Chief Information Officer of DHS and respective Information System Security Manager. These security controls allow for information critical to the posture of DHS to be protected. The PII contained in HSVAC is treated with the same level of sensitivity and criticality as the Sensitive But Unclassified (SBU) information.

Section 3.0 Retention

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

3.1 What is the retention period for the data in the system?

User specific information, including PII collected during the registration process will be destroyed or deleted six (6) years after the user account is terminated or when this information is no longer needed for system auditing and security purposes, whichever is later. Information pertaining to training and training requests will be destroyed five (5) years after the completion of the HSVAC program.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes; NARA has approved the retention schedule for FEMA and retention for the HSVAC complies with the NARA approved record retention schedule contained in FEMA Manual 5400.2 (NARA GRS-1 29a(2), GRS-1 29b and GRS-1 24 (6)).

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

This information is retained for the purpose of confirming the identity of registrants, to support the training efforts, and to allow for auditing of system usage and training activities.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

HSVAC information is used to support FEMA NPD preparedness, training and exercises.

4.2 For each organization, what information is shared and for what purpose?

Generally, information mentioned in section 1.1 is shared with HSVAC administrators to verify the identity and eligibility of individuals requesting assess to HSVAC. The HSVAC administrators are comprised of FEMA staff members and contractor support personnel. In addition, authorized users request training through HSVAC. The information shared for training requests includes the user's name, email address, and phone. HSVAC information is used to support NPD preparedness, training and exercises. Information concerning training and exercises may be shared DHS wide if there is a need to know within the scope of duties.

4.3 How is the information transmitted or disclosed?

If there is a need to know within the scope of duties, communication and information transfers are performed using SSL 128-bit encryption to protect user and system information.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The identified risk associated with the disclosure of PII consisted of administrative or support personnel acting in a malicious and irresponsible fashion. This has been mitigated through the use of audit trails and syslog logs which record each action performed by the users in the system. These logs are periodically reviewed to ensure that users with administrative privileges behave in a way that is consistent with the Rules of Behavior set for HSVAC.

Section 5.0 External Sharing and Disclosure

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

5.1 With which external organizations is the information shared?

Information may be shared with authorized HSVAC users that have been assigned to the state and local HSVAC SAA/UAWG and Training Assistance (TA) provider roles.

5.2 What information is shared and for what purpose?

Generally, information mentioned in section 1.1 is shared to verify the identity and eligibility of individuals requesting assess to HSVAC. In addition, authorized users request training through HSVAC. The information shared for training requests includes the user's name, email address, and phone.

Information is shared as required to approve service design and training service delivery requests and to manage lower-level accounts in the same SAA/UAWG State or Urban area or TA provider.

5.3 How is the information transmitted or disclosed?

If there is a need to know within the scope of duties, information will be transmitted through the HSVAC secure web application which uses Secure Sockets Layer (SSL) 128-bit encryption.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

All HSVAC users, including SAA/UAWG State or Urban area and TA providers must comply with the HSVAC Rules of Behavior which addresses all aspects of their access, use, security, and permissible further dissemination of the data within the HSVAC system.

5.5 How is the shared information secured by the recipient?

All HSVAC users, including SAA/UAWG State or Urban area and TA providers must comply with the HSVAC Rules of Behavior which addresses all aspects of their access, use, security, permissible further dissemination of the data and destruction of HSVAC data when no longer needed.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

No specific training is required by HSVAC. HSVAC members are DHS officials and emergency response providers. In the general course of performing their assigned duties, DHS officials and contractor staff are required to attend Security Awareness training.

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

The risks to HSVAC PII were identified through a review and analysis of process flow and controls conducted by HSVAC developers, Information Systems Security Officer (ISSO) personnel, administrative personnel, and the HSVAC System Owner. In addition, in accordance with the DHS Sensitive Systems Handbook, HSVAC ensures effective security controls and authentication. By enforcing system policies, Rules of Behavior, system and application settings, and strong passwords, HSVAC mitigates risks of disclosure of PII when shared.

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? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Notice is provided by the General Information Technology Access Account Records System (GITAARS) DHS/ALL-004, May 15, 2008, 73 FR 28139 System of Record Notice (SORN). This PIA serves as notice regarding how DHS will use PII that may be collected and used by the HSVAC. Additionally, when logging into HSVAC users are notified that they are accessing a government system, that all access is subject to monitoring, and that there is no expectation of privacy in the course of the use of the system.

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

Yes. Individuals can exercise their option to not register into the HSVAC system. Registration into the HSVAC system requires individuals to input certain PII into the system. If an individual declines to provide information necessary to register for access the system, he/she will be denied access to the HSVAC and the scheduling, coordination, and management of first responder training provided to state and local government entities and organizations through the application.

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

By virtue of proceeding with the registration process, users implicitly agree that their personal information will be used to verify their identity. The information will not be used for any other purpose. Thus, users are not provided opportunity to consent to additional uses of their information as no other uses are appropriate.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Access to HSVAC is voluntary. Users must agree to the terms of system use, monitoring and Rules of Behavior. This PIA and the system of records notice provides general notice of the type of information that will be used in HSVAC and the limited purpose for that use.

Section 7.0 Individual 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 which allow individuals to gain access to their own information?

Users are capable of reviewing all PII that they provide by selecting the "Update Account Information" link found at the upper right hand of the HSVAC. Through this link, users are also able to correct or update any information that may have been originally entered incorrectly at the time of registration or information that may have changed since the time of registration. If users are unable to access their records electronically, they may follow procedures outlined in FEMA's and DHS' Privacy Act regulations, 44 CFR Part 6 and 6 CFR Part 5. Requests for Privacy Act protected information must be made in writing and clearly marked as a "Privacy Act Request." The name of the requester, the nature of the record sought, and the required verification of identity must be clearly indicated.

Requests should be sent to: FOIA Officer, Records Management, Federal Emergency Management Agency, Department of Homeland Security, 500 C Street, SW, Washington DC 20472.

7.2 What are the procedures for correcting erroneous information?

Two different processes are in place that allows a user to correct erroneous information entered upon the time of registration. Users are allowed to log into the HSVAC system and update their personal information using the "Update Account Information" link and corresponding fields that will populate the screen. Users are also capable of calling the Support Services Center that has been established for the HSVAC system. When receiving an account restoration, if the user's identity has been verified through established means, the user may then request the help desk technician or senior technician to update their account information to reflect accuracy.

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

User manuals for the HSVAC system have been distributed and made available to each prospective user. In these user manuals, the instructions for how to correct erroneous account information are available for easy reference to each user. Should a user have any questions about the information contained in the user manuals they are able to call the Support Services Center established for HSVAC and after the user's identity is confirmed, they will be able to update the necessary fields.

7.4 If no redress is provided, are alternatives available?

Due to the limited amount of personal information that is supplied by the individual during registration, the ease of the access of these files, and the capability of the user in correcting this

information, no formal redress is necessary. The individuals who have access to the HSVAC have access to their records and the capability to seek corrections or amendments at any time.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

As stated previously in sections 7.1 and 7.2, the users are fully capable of accessing and correcting their records in this system. Procedures are outlined in the HSVAC User Manual. See section 7.3. Since users of the HSVAC system have virtually unlimited access to their records and the capability of making appropriate corrections/amendments at anytime, redress alternatives are not necessary.

Section 8.0 Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

HSVAC operates in a secured environment and physical access is limited to system administrators, database administrators, ISSOs and other individuals that require access in order to perform their duties in managing, upgrading, and securing the system. HSVAC application administrators and users access the system using a secure web interface. No unauthorized users are permitted access to system resources.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

HSVAC is securely hosted and managed by contractor staff. In addition to operations and maintenance tasks, contractor staff perform application development, security monitoring and ISSO duties. All contractors are subjected to vetting requirements for suitability and a background investigation in accordance with the DHS Sensitive Systems Handbook and contractors have signed appropriate non-disclosure agreements and agreed to handle the information in accordance with the Privacy Act of 1974, as amended. Only those contractors with a verified need to know and approved vetting will be granted access to the HSVAC system.

8.3 Does the system use “roles” to assign privileges to users of the system?

HSVAC uses role-based access controls (RBAC) to control access to both data and functions so that each user is granted the minimum amount of access to the system that is necessary according to his/her

official role.

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

The system is secured against unauthorized use through the use of a layered, defense-in-depth security approach involving managerial, operational and technical controls and security safeguards as documented in the HSVAC System Security Plan (SSP). Because HSVAC may provide sensitive but unclassified information, access to HSVAC is limited to Homeland Security Officials, emergency first responders and training providers that have been authorized and validated by HSVAC administrators. A secure online registration form is used to gather member applications.

To provide accountability and traceability for all actions performed, HSVAC assigns a unique UserID and password to each user and administrator. HSVAC is a role based application and access to data is restricted by the user's role within the system. Separation of duties is enforced with system administrators and contractor personnel.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

HSVAC assignments of roles and the levels of access are reviewed on an annual basis in accordance with the HSVAC System Security Plan (SSP). The SSP describes in detail all measures taken to ensure HSVAC complies with Federal IT standards as dictated by the FISMA. Additionally, all access attempts are logged on the HSVAC server for audit purposes.

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

All user actions are logged and periodically reviewed to ensure that misuse of the system does not occur. Separation of duties is in place to ensure that users who have a functional administrative account in the system are incapable of altering/auditing the log files.

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

Privacy training is provided based upon risk. High risk positions, which include the application developers, TA Managers and support personnel such as data base administrators and system administrators, receive privacy training through the DHS Security Awareness Training annual refresher course.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes, HSVAC has received Authority to Operate (ATO) which is valid through June 10, 2011.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Security controls are in place to protect the confidentiality, availability, and integrity of the data, including role-based access controls to enforce a strict need to know policy. Each user is given a unique login name and password and audit trails are maintained and monitored to track user access and detect any unauthorized use. All HSVAC system users must agree to the system Rules of Behavior.

The managerial, operational and technical controls implemented to protect the confidentiality, integrity and availability of HSVAC and its information comply with the requirements of the DHS Sensitive Systems Handbook and FISMA. These controls are reviewed annually through a Security Test and Evaluation (ST&E), Security Assessment and Annual SP800-53A Self Assessment. Any control weaknesses identified will be remediated through the use of a Plan of Actions and Milestones (POA&M).

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, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

The HSVAC system was built from the ground up by K2Share. K2Share is a consulting company dedicated to providing information technology support services, secure system hosting, security and C&A solutions to government and corporate clients.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Security and privacy requirements were analyzed based on FIPS-199 methodology. FIPS-199 methodology categorizes a system as High, Medium, or Low, depending on how important the function is to the agency. The result of that analysis was that the HSVAC system was rated as Moderate for data integrity and confidentiality. All security controls are applied in accordance with this rating.

Data integrity, confidentiality, and security were a vital part of the system design. By utilizing a

role-based system, only authorized individuals with a valid need to know have access to HSVAC. All hardware systems and software were configured to protect the data from improper access and to comply with FISMA and all other applicable security and privacy policies mandated for Federal IT systems.

9.3 What design choices were made to enhance privacy?

Privacy was considered at the onset of the development of HSVAC. Role-based access ensures that only users with authorization have access to sensitive or PII.

Responsible Officials

John A. Sharetts-Sullivan
Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature Page

Original signed an on File with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security