Privacy Impact Assessment
for the

FireGround Compass

April 1, 2009

Contact Point
Gregory Price
TechSolutions
Science and Technology Directorate
(202) 254-6720

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security Science and Technology Directorate (DHS S&T) TechSolutions Program contracted with G&H International Services, Inc. to perform operational testing and evaluations on the FireGround Compass for first responder firefighter applications. Halcyon Products designed the FireGround Compass, a navigational device that helps firefighters reestablish their orientation within a burning or smoke-filled building should they become lost or disoriented. The purpose of this project was to test the features, functions, and operational readiness of the FireGround Compass through human testing of the equipment. S&T conducted a PIA for this project because G&H International collected the personally identifiable information (PII) of firefighter volunteers during the testing of the device.

Overview

Title 3 of the Homeland Security Act assigned S&T the responsibility for conducting research in support of the Department's mission. Under Subchapter 3 §182, "the Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department."

The FireGround Compass is a navigational device that enables firefighters, their exterior sector officers, and the fire-ground commander to navigate a burning building or area as they battle interior structural fires. Unique features of this device include: an LED light that illuminates the compass and building points, a rectangular bezel with four corners that represents an incident building, and an inner round bezel that rotates to mark the position of the command post or point of entry. These features enable firefighters to reestablish their orientation within a smoke-filled or burning building should they become lost or disoriented, allowing them to escape a building quickly in emergency situations. The device helps keep all members at an incident oriented with the burning structure, the overall scene, and the fire-ground commander. This can give on-scene crews more confidence to do their jobs safely and efficiently.

The FireGround Compass project supported S&T's research mission by performing prototyping, operational tests, and evaluations on a device that addressed the capability gaps and needs of first responders, specifically firefighter units. The purpose of the project was to test features, functions, and operational readiness of the FireGround Compass in a variety of settings. The specific objectives of the tests were to evaluate the device's:

- Resistance to water intrusion;
- Impact strength (ruggedness/survivability to typical drops);
- Heat resistance properties;
- Full range of mechanical adjustments (durability);

- Resilience to typical structural fire flame/heat exposure;
- Legibility of black box and bezel markings in low ambient lighting/obstruction;
- Legibility and proper operation under icing conditions;
- Ease of accessing, stowing, and carrying while donned in standard turnout gear, dry, wet, and outer butyl rubber gloves; and
- Usability in a live fire/smoke chamber using SCBA and structural protective ensemble.

Testing

S&T funded G&H International Services, Inc. to conduct operational tests and evaluations on this equipment in partnership with Eastern Kentucky University (EKU) and Richmond (Kentucky) Fire Department to determine the utility and benefits of deploying the FireGround Compass to firefighters. The tests focused on establishing the benefits of deploying the FireGround Compass to firefighters and determining the equipment's capabilities in an operational environment. Upon successful completion of the tests, G&H International and EKU compiled a final report evaluating the device for S&T, which S&T will provide to educate potential customers/users. The report documented the results from the operational tests.

During the series of tests, G&H International and EKU testing staff deployed the FireGround Compass to three certified firefighter volunteer test subjects, who served as the user community proxy for operational tests. During testing, all volunteers were employees of the City of Richmond Fire/Rescue Department. In accordance with the human subjects research regulations set forth in 45 CFR 46, the Institutional Review Board (IRB) of EKU approved the use of human test subjects for the research. Testing staff carried out the tests at multiple venues at EKU and the Fire Training Center of the Richmond Fire Department to test the performance of the device in both laboratory and simulated environments.

During the operational tests, the volunteers donned a standard fire fighting ensemble, worked in environments that simulated a real fire, and navigated the space using the FireGround Compass. G&H International and EKU testing staff recorded each test, capturing audio and video recordings of volunteers, to make determinations regarding the functionality of the device and analyze the test results and data. The testing staff interviewed the volunteers to provide observations and feedback on the utility of the device. The testing staff collected demographic data about volunteers (volunteer's height, weight, vision, and years of experience) to support the experiment, but they did not collect contact information or any additional personally identifiable information. The testing staff maintained, owned, and controlled all information collected during the field test. The testing staff anonymized the volunteer's personally identifiable information prior to publication of any final reports or results. G&H International and EKU did not include names or pictures of volunteers in any publications.

Participants

The FireGround testing included the following participants:

1. Halcyon Products, Inc. developed and provided the device to be tested. Halcyon provided technical support and training to the volunteer firefighter test subjects on how to properly use device.

2. G&H International assembled a team of subcontractors from EKU to design and execute each test. G&H International also provided a Safety Officer who ensured safety issues were addressed for each test performed.

3. EKU coordinated and provided the facilities to test the equipment. EKU also led and directed all testing activities. The EKU IRB approved the human testing activities.

4. The City of Richmond Fire/Rescue Department provided the volunteer test subjects that participated in the tests. The Fire/Rescue Department also provided equipment and facilities, including the burn building, smoke house, and fire trucks necessary to complete testing.

5. S&T provided funding and overall program management and participated as observers in the operational tests. S&T assisted in program planning and organizing testing events. Their participation was strictly to observe and evaluate the features, functions, and operational readiness of the FireGround Compass.

Section 1.0 Characterization of the Information

The following subsections 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?

Testing staff from G&H International and EKU collected demographic data (height, age, vision and years of experience) from the volunteers to evaluate the performance of the device across a broad range of physical and professional characteristics. The testing staff video taped the tests, capturing images and audio recordings of volunteers. The testing staff also interviewed volunteers at the conclusion of the tests to obtain feedback on the performance of the device in test settings. The testing staff anonymized the volunteer's PII prior to publication of any final reports or results. G&H International and EKU did not include names or pictures of volunteers in any publications.

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

Testing staff collected information directly from the volunteers through surveys and interviews. Video cameras captured the images and audio recordings of the volunteers during the tests.

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

The project was an operational testing and evaluation of a device that firefighters may deploy for their applications. G&H International and EKU testing staff collected information from the firefighter volunteers to adequately evaluate the device and compile a comprehensive final report on which future deployment of the device may be based.

1.4 How is the information collected?

Test subject volunteers transmitted demographic data (i.e., years of experience and vision) to the EKU Test Administrator via email. The EKU Test Administrator deleted the emails once the demographic information was collected. G&H International and EKU testing staff also collected volunteers' feedback and observations through surveys and interviews. Testing staff videotaped the volunteers during the tests and captured video and audio recordings. Prior to data collection, volunteers signed informed consent forms for the collection of information and video/audio recordings.

1.5 How will the information be checked for accuracy?

Individuals verified the accuracy of all the information collected at the time of collection.

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

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorized the Science and Technology Directorate to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T was authorized to collect information, as appropriate, to support R&D related to improving the security of the homeland.

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

The risk associated with collecting this information was that unauthorized users may have had access to the information or used the information for unauthorized purposes. The testing staff mitigated this risk by anonymizing all information in the final reports and publications. These reports detail what data was collected but do not include actual data related to any volunteer's height, weight, etc. The testing staff gave volunteers unique identifiers and blurred all images of volunteers. Once testing staff

determined that the information was no longer needed, they destroyed all information. Additionally, testing staff limited access to information to only authorized personnel with an appropriate "need to know."

Furthermore, all volunteers signed informed consent forms and received a full briefing prior to initiation of tests. The briefing explained which information the researcher would collect and how the information would be used. In addition, researchers explained that they would anonymize volunteer PII before including anything in a final report.

Section 2.0 Uses of the Information

The following subsections 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.

G&H International and EKU testing staff collected information in order to enable them to evaluate the performance of the device across a broad range of physical and professional characteristics. Demographic data, including height, age, vision and years of experience, were important factors in evaluating the utility of the device. There were no other uses for the information. The testing staff anonymized all PII—names and other identifying information—in final reports and publications and destroyed all other information—video and audio—once they determined it was no longer needed.

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

The testing staff manually analyzed the information collected and compile a final report. The final report will be used to verify the device functions as reported under simulated operational conditions.

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

The testing staff did not use commercial or publicly available data during the tests.

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.

The privacy risk associated with the uses of the information was that unauthorized users may view stored information or use the information for unauthorized purposes. To mitigate this risk, only authorized personnel with a "need-to-know" have access to information. Adequate safeguards (physical and technical) were employed to protect information from unauthorized access. Authorized testing staff placed all videos and hard copy documents in a single room with video surveillance, badge and PIN lock doors and locked safes and file cabinets. Electronic documents were maintained in the same room on a

network connected computer. Both computer and network access were protected by user name and password privileges. Document access was restricted via document access controls. Only those test team individuals with a need to know were granted access to the room, computer network and files.

Section 3.0 Retention

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

3.1 What information is retained?

S&T did not collect, receive, or retain any personal information. G&H International and EKU testing staff collected and retained volunteer demographic information, including: name, height, weight, years of experience, vision, and test feedback. At the conclusion of the project, S&T staff received a final report containing anonymized information. All PII collected by the testing staff during the test was destroyed.

3.2 How long is information retained?

S&T did not retain any PII before, during or after the test. G&H International and EKU testing staff retained information until a final report was compiled. Once final analyses and evaluations were made and published, testing staff destroyed all PII. The testing staff anonymized all PII in all published reports. At the conclusion of the project, S&T received a copy of the anonymized final report.

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

Yes. The S&T Records Retention Officer approved the use of General Records Schedule 20 and 24 to cover all programs files.

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

The information collected was stored until testing staff produced a final report. During that time, a risk associated with data retention was the unauthorized access of the information. To mitigate this risk, testing staff employed all appropriate physical and technical safeguards to secure information. This included locking all information in a safe when not used and using firewalls and encryption techniques to protect any information stored on electronic devices.

Section 4.0 Internal Sharing and Disclosure

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

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

S&T did not receive or have access to any of the PII. Only G&H International and EKU testing staff working on the FireGround Compass project had access to PII to evaluate the features, functions, and operational readiness of the device for firefighter applications. At the conclusion of the project, S&T only received the anonymized final report. G&H International and EKU testing staff did not share any PII with any other internal organizations.

4.2 How is the information transmitted or disclosed?

S&T did not receive or have access to any PII; therefore, S&T did not transmit or disclose any information. G&H International and EKU did not transmit any PII to S&T or any other internal organization.

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.

S&T did not share the information with any internal organizations.

Section 5.0 External Sharing and Disclosure

The following subsections 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 organization(s) is the information shared, what information is shared, and for what purpose?

The S&T staff did not have access to the information. The two external parties—G&H International and EKU testing staff—collected information to evaluate and make determinations on the utility and functionality of the device. G&H International and EKU did not share the information with any other organizations external to DHS or themselves.

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 DHS.

S&T did not have access to or receive any PII and, therefore, did not share the information with any external organizations. G&H International and the EKU research staff produced a final report, in which all PII was anonymized, and made the report available to first responders via R-Techs FirstResponder.gov website.

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

Only G&H International and EKU research staff collected, received, or had access to PII. No PII collected was shared outside the department; only authorized testing staff received or had access to the information. Test subject volunteers transmitted demographic data (i.e., years of experience and vision) to the EKU Test Administrator via email.

S&T shared the final report, in which all PII was anonymized, outside the Department with first responders via the FirstResponder.gov website. FirstResponder.gov is a DHS S&T system that has received certification and accreditation from the DHS S&T CIO.

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

S&T did not collect PII during the test event. However, two external organizations, G&H International and EKU, collected and had access to the PII, which they did not share externally. Instead, they produced a final report, which S&T shared externally with first responders via the FirstResponder.gov website. The privacy risk associated with this external sharing is that volunteers may be identifiable. To mitigate this risk, G&H International and EKU anonymized any PII before including such data in the final report.

Section 6.0 Notice

The following subsections 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?

Testing staff provided detailed notice to volunteers prior to data collection, and all volunteers signed informed consent forms prior to the initiation of the research.

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

Volunteers participating in the research were under no obligation to provide information. Each volunteer had the right to decline providing information if they so chose.

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

Yes. Prior to data collection, volunteers signed informed consent forms that clearly stated the uses of the information.

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.

The testing staff provided adequate notice to the volunteers in the informed consent form, which volunteers signed prior to data collection. The consent form allowed researchers to collect each participant's data, photograph, and video images. The testing staff also notified all volunteers of their participation in the research both orally and in writing.

Section 7.0 Access, Redress and Correction

The following subsections 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?

The researchers allowed all test subjects to access information collected during the test. Volunteers gained access to information by contacting the Test Director and/or the test Data Recorders. Testing staff notified volunteers of such mechanisms during the initial briefing, prior to the start of the project.

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

Testing staff collected information directly from the volunteer test subjects. Testing staff gave volunteers the opportunity to correct any inaccurate or erroneous information at the time of data collection. After researchers compiled the test results and feedback, they provided volunteers the opportunity to review their own information for accuracy.

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

The testing staff notified the volunteers of procedures for correcting their information during the initial briefings, prior to starting the project. Testing staff collected information directly from the volunteer test subjects and provided individuals the opportunity to correct inaccurate or erroneous information at the time of collection.

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

Testing staff provided appropriate redress procedure to the volunteers, as described above.

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

The privacy risk associated with access and redress was that researchers could record incorrect information about individuals. To mitigate this risk, testing staff gave volunteers the opportunity to review and correct their own information.

Section 8.0 Technical Access and Security

The following subsections 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?

Only authorized testing staff working directly on this project had access to the system. Two layers of access control (badge and ID#/PIN number) and a video surveillance system protected the workstation location. Username and password privileges protected the computer and network. Access to documents required file-level permissions. The procedures were not documented.

8.2 Will Department contractors have access to the system?

Yes. Testing staff from G&H International and EKU had access to the information collected.

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

All DHS S&T personnel working on the project received initial and annual privacy training. S&T provided Web-based privacy awareness training to all G&H International personnel and EKU subcontractors involved in the project. The training provided guidance to testing staff on how to safeguard, store, and handle PII properly.

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

The S&T OCIO determined that a C&A was not required for the project.

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

The following technical safeguards and auditing measures were used to prevent misuse of data:

- An internal firewall protected the network to which the workstation connected.
- A secondary firewall protected all servers, which included e-mail servers and departmental servers.
- Multi-tiered antivirus, antimalware, and anti-spam software and program packages protected the network, also.

- The EKU IT staff maintained and continuously audited the network, which provided alerts if it identified questionable activity. The EKU IT staff initiated a manual process to monitor and investigate any suspicious activity.
- Network security procedures and practices are audited each year by an external agency.

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 privacy risks associated with technical access and security included unauthorized access to information or inappropriate uses of the information. Testing staff mitigated this risk by limiting access to authorized program staff and ensuring that information was used in concurrence with the documented purposes. Testing staff mitigated the risk by ensuring that all staff employ appropriate safeguards as previously discussed. Further, testing staff employed encryption technology to secure all transmissions.

Section 9.0 Technology

The following subsections 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 What type of project is the program or system?

The project involved development, prototyping, testing, and evaluation of a first responder device that addressed capability gaps and needs of the firefighter community. The objective of the project was to test the unique features, functions, and operational readiness of the FireGround Compass for first responder applications.

9.2 What stage of development is the system in and what project development lifecycle was used?

Halcyon Inc. developed and manufactured this device. S&T tested its utility and functionality for operational deployment for first responder applications.

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

No. As a navigation device, the technology design enabled firefighters to reorient themselves in a smoke-filled or burning building.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security