Privacy Impact Assessment
for the

24x7 Incident Handling and Response Center

March 29, 2007

Contact Point
Michael Witt
National Cyber Security Division
Department of Homeland Security
(703) 235-5160

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The 24x7 Incident Handling and Response Center ("24x7") focuses on ways to gather cyber information prior to attacks and to use that information to prevent attacks, protect computing infrastructure, and respond/restore where attacks are successful. 24x7 serves as a communication hub for the United States Computer Readiness Team (US-CERT) program, issuing regular security and warning bulletins, serving as a gateway for public contribution and outreach, and also serving as a ticketing center through which tasks may be delegated out to the various US-CERT programs.

Introduction

The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The Federal Computer Incident Response Center (FedCIRC), established in Oct 1996 by the National Institute for Science and Technology (NIST) as a pilot program and taken over by the General Services Administration (GSA) in October 1998 as an operational entity, formed the initial nucleus of the US-CERT when DHS was established in March 2003.

The 24x7 Incident Handling and Response Center ("24x7") focuses on ways to gather cyber information prior to attacks and to use that information to prevent attacks, protect computing infrastructure, and respond/restore where attacks are successful. The program utilizes a number of tools to achieve this objective including: (1) the US-CERT Portal ("Portal"), which is the nation's clearinghouse for cyber-security risk data, and services the Federal civilian government, State, Local, and tribal governments and the private sector; (2) a call center whereby individuals from the private and public sectors may contact US-CERT to report a cyber-related incident; and (3) an online Incident Reporting System, which has the same function as the call center.

24x7 also serves as a trouble ticketing system for US-CERT. Individuals from the private and public sector may contact US-CERT through 24x7, whereby the individual's contact information and the nature of the concern is collected. If the problem is one that cannot be addressed through 24x7's resources, a trouble ticket is created and notification is sent to an appropriate program within US-CERT to be handled.

When an incident has been reported to 24x7, a follow-up assessment of the reported incident and the event is handled within 24x7. If the nature of the problem is one that cannot be addressed through 24x7's resources, the incident data as well as the reporting individual's contact information is passed on to the appropriate program within US-CERT or the CERT Vulnerability program.[1] If the incident data is

[1] The CERT Vulnerability Analysis Project has been established to understand the complete behavior of malicious code and other attack tools in order to develop countermeasures or recommend courses of action for combating malicious code that may be used to target or exploit the US Federal Government and/or Critical Infrastructure. To this end, CERT Vulnerability works closely with cyber security experts in the federal government, state/local governments, intelligence community, critical infrastructure owners/operators, public and private sectors. This CERT Vulnerability is made up of two initiatives that constitute the investment programs: (1) Artifact Analysis/Catalogue ("Artifact Catalogue") and (2) Software Vulnerability collection and strategic analysis ("Software Vulnerability Analysis"). The Artifact Catalogue and the Software Vulnerability Analysis are separate data systems. Artifact Catalogue involves collecting and cataloguing malicious code. This allows computer security professionals to refer to a single source of malicious code analysis; the Software Vulnerability Analysis is focused on sharing analysis with professionals who need to know in public and private sectors.

submitted to EINSTEIN, the contact information and incident data is maintained within the 24x7 database. If the incident data is submitted to CERT Vulnerability, the incident data and any accompanying contact information is stored in a secure vulnerability database until there is no longer any security or business purposes for retaining such data.

24x7's Cyber Security Bulletins and Cyber Alerts provide the following information and services to respond to six weaknesses consistently recognized by GAO and OMB, specifically the following:

1) Worm Detection: Sharing and collaborating on IT incidents, threats, and vulnerabilities produces a sophisticated picture of attacks across the Federal .gov domain. The US-CERT provides this information directly to network administrators for the benefit of department and agency systems protection.

2) Anomalous Network Activity: The capability offers directly to the department and agency administrators an easy to understand picture on priority emergencies and needs for both in and outbound traffic. In the absence of such information, administrators must continue to rely on insufficient information to leverage scarce resources and to protect their systems.

3) Configuration Management: The US-CERT will be able to provide counsel on configuration management options. Configuration challenges are fast becoming one of the most difficult problems for agency administrators.

4) Trends Analysis: The US-CERT uses the information collected and analyzed to generate a cross-governmental trends analysis. The analysis offers to departments and agencies an accurate and aggregate picture on the health of the Federal.gov domain. The information is offered in real-time, and may include an assessment of anomalous amounts of network traffic across the .gov domain or in some cases, within a single agency. The data can also offer an aggregate comparison on the health of the Federal .gov domain as compared to the Internet or even portions of the national network.

Through 24x7 US-CERT better coordinates its communication and information collection to better protect against cyber-security threats. This PIA discusses the role of 24x7 and the information 24x7 collects.

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?

24x7 gathers information regarding cyber-related incidents such as attempted breaches, isolated malicious code, which includes time, date, and IP addresses, through reports from private individuals, companies, and federal, state, and local governments and uses that information to prevent attacks, protect computing infrastructure, and respond/restore where attacks are successful. In addition to the cyber-related incident information itself, contact information from the submitting individual, organization or

agency is retained. This consists of name, phone number and/or e-mail address with which, if need be, to contact the person.

The information gathered through the call center and the Incident Reporting System, allows 24x7 to generate Cyber Security Bulletins (strategic analysis) and day-to-day alerts and warnings via our Cyber Alerts where critical threats, vulnerabilities, and incidents are discovered. 24x7 also serves as a ticketing system. Individuals from the private and public sector may contact US-CERT through 24x7, whereby the individual's contact information and the nature of the concern (i.e. new virus activity, a software malfunction or a breach of data due to malware) is collected. If the problem is one that cannot be addressed through 24x7's resources, a trouble ticket is created and notification is sent to the appropriate program within US-CERT for handling (EINSTEIN or CERT Vulnerability).

Once an incident has been reported to 24x7, a follow-up assessment of the reported incident and the event is handled within 24x7. If the nature the problem is one that cannot be addressed through 24x7's resources, the incident data as well as the reporting individual's contact information is passed on to the appropriate program within US-CERT to be handled (the EINSTEIN Program PIA published September 2004) or the CERT Vulnerability program. If the incident data is submitted to Einstein, the contact information and incident data is maintained within the 24x7 database. If the incident data is submitted to CERT Vulnerability, the incident data and any accompanying contact information is stored in a secure vulnerability database until there is no longer any security or business purposes for retaining such data.

1.2 From whom is information collected?

Information for 24x7 is collected from individuals in both the public and private sector who voluntarily report on incidents, vulnerabilities, and phishing scams or voluntarily contact 24x7 for assistance with a cyber-related concern. The sources of information in this system principally include federal government network security managers and those in the private sector that are interested and willing to contribute to the catalogue of incidents and/or our analysis of that incident. US-CERT is, for example, also acquiring information from computer emergency response teams across the nation.

1.3 Why is the information being collected?

24x7 collects only that information which is necessary to fulfill the US-CERT's homeland security mission: to raise awareness about malicious code, to prevent computer attacks against the nation cyber vulnerabilities, and to respond and restore systems where attacks are successfully launched. The cataloguing and analysis of cyber-related incidents permits public and private sectors to develop protective measures to prevent/protect from such attacks, and also to develop response/restoration strategies where attacks are successful. 24x7 does not collect information beyond that which is needed to catalogue the cyber-related incident and/or to contact the reporting individual to further assist with the individual's cyber-related concern.

In addition, the information gathered through the call center and the Incident Reporting System, allows 24x7 to generate Cyber Security Bulletins (strategic analysis) and day-to-day alerts and warnings via our Cyber Alerts where critical threats, vulnerabilities, and incidents are discovered. 24x7 also serves as a ticketing system.

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

The Federal Information Security Management Act established the requirement for a federal information security response center whose function OMB designated first FedCIRC then US-CERT to handle. Also, the National Strategy to Secure Cyberspace discusses the establishment of a National Cyberspace Security Response System, a National Cyberspace Security Threat and Vulnerability Reduction Program, Securing the Government's Cyberspace, and handling International Cyberspace Security Cooperation; FedCIRC was expanded into the US-CERT to meet these priorities.

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.

There is a risk associated with the collection of personally identifiable information. While this is a significant risk, the collection of the reporting individual's contact information allows 24x7 analysts to verify reported data, and engage in follow-on discussions regarding the cyber-related incident. To mitigate this risk, US-CERT has integrated robust security expectations into our risk management plans and routinely tests the security of our systems. In addition, US-CERT continually reviews developments affecting privacy with the Privacy Office and Preparedness' Disclosure Officer. Further, US-CERT has implemented best practices such as auditing to defend against misuse of the data and routinely monitor those with access to the information. In addition, in accordance with the DHS Sensitive Systems Handbook, Preparedness ensures effective security controls and authentication. By enforcing system policies and settings and strong passwords, Preparedness protects the privacy of systems which promote or permit public access and the integrity of the data itself. Further, US-CERT collects the minimum amount of information necessary to address the reported incident and conduct follow-up calls, if necessary, with the reporting individual.

Also, any contact information is not searchable. Contact information is only secondary data shared with a researcher who feels follow-up information would help analysis of an incident or code. In the case that specific code or incident information is required to be shared beyond US-CERT, contact information is scrubbed to eliminate any potential transmission of such data.

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 information gathered through the call center and the Incident Reporting System, allows 24x7 to generate Cyber Security Bulletins (strategic analyses) and day-to-day alerts and warnings via our Cyber Alerts where critical threats, vulnerabilities, and incidents are discovered.

Personal information is used for follow-up research by a CERT program where necessary or for those subscribing to a US-CERT bulletin.

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")?

No. US-CERT only analyzes the incident data to assess whether there is a pattern of attack. Contact information is not analyzed in any way.

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

Where individuals voluntarily provide their name, e-mail, and phone number (such as with incident reporting or a trouble ticket), US-CERT may under limited circumstances call these individuals to verify the security data or to follow-up on a trouble ticket submitted by the individual. US-CERT does not maintain records on individuals. The contact information is not maintained as a separate contact database. The information is considered to be accurate because it is being received from individuals themselves. Individuals subscribing to a US-CERT bulletin have an interest in actually receiving the bulletin and individuals submitting incident or code information are often willing to provide further information in order to better support the information security community. However, because the contact information is not required to analyze the code or incident—only to follow-up—if contact information is inaccurate no consequences result.

In order to assess the veracity of the reported incident, US-CERT first obtains the details of the incident from the reporting individual. The next step is to contact the owner of the affected system (i.e. Microsoft, Adobe, etc.) to notify the owner and allow the owner to assess the system to determine whether the incident has occurred. It is the owner's responsibility to verify the incident. US-CERT's role, once the incident is verified, is to prepare a report to notify users of the incident.

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.

As discussed in Section 2.3, it is the researcher's responsibility to verify the incident data if necessary. US-CERT's role, once the incident is verified, is to prepare a report to notify users of the incident.

In accordance with the DHS Sensitive Systems Handbook, Preparedness ensures effective security controls and authentication. By enforcing system policies and settings and strong passwords, Preparedness protects the privacy of systems which promote or permit public access and the integrity of the data itself. It should be repeated that the contact information is helpful to the US-CERT mission and US-CERT encourages submission of incident and malicious code data, but the contact information is not primary mission information for US-CERT. Contact information absolutely may not be released beyond US-CERT.

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?

Until the records in the system have a NARA-approved disposition schedule, the records must be considered permanent and nothing may be deleted.

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

An approval request is in process. DHS / Preparedness is currently working with the DHS Senior Records Officer to develop a disposition schedule which will be sent to NARA for approval.

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

The information is needed for historical reference purposes to analyze the cyber-related incident and/or provide assistance with respect to the trouble ticket. US-CERT is currently working with DHS Senior Records Officer to finalize a mission-related retention policy. Until such time as the policy is developed, the data will be retained for the duration of the program, in accordance with NARA Guidelines.

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?

Incident data and contact information are never shared outside of US-CERT. While all internal DHS organizations have access to the general Cyber Security Bulletins and Cyber Alerts, the personal information gathered from the reporting individual is only used within US-CERT. Further, any information gathered through the ticketing system is only used within US-CERT. The reporting source of the information is not released.

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

Incident data and contact information are never shared outside of US-CERT. No personally identifiable information is shared with internal organizations. Any information shared relates only to the Cyber Security Bulletins and Cyber Alerts which are the culmination of the analyses of several incident

reports. Further, any information gathered through the ticketing system is only used within US-CERT. The reporting source of the information is not released.

4.3 How is the information transmitted or disclosed?

Incident data and contact information are never shared outside of US-CERT. The reporting source of the information is not released. Information regarding the cyber-related incident is transmitted via the Cyber Security Bulletins and Cyber Alerts. Further, any information gathered through the ticketing system is only used within US-CERT.

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

Incident data and personal information are never shared outside of US-CERT. No personally identifying information is shared throughout the Department. Only US-CERT authorized users can see the personal contact information gathered through the call center, Incident Reporting System and ticketing system, and only when the US-CERT authorized user has the need to know both the incident and contact data.

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?

None. Federal civilian agencies, state and local government, and the private sector have access to the Cyber Security Bulletins and the Cyber Alerts; however only US-CERT authorized users can see the personal contact information gathered through the call center, Incident Reporting System, and ticketing system.

5.2 What information is shared and for what purpose?

Not applicable. No contact information is shared outside of US-CERT. Federal civilian agencies, state and local government, and the private sector have access to the Cyber Security Bulletins and the Cyber Alerts; however, only US-CERT authorized users can see the personal contact information gathered through the call center, Incident Reporting System, and ticketing system.

5.3 How is the information transmitted or disclosed?

The reporting source of the information is not released. Only US-CERT authorized users can see the personal contact information gathered through the call center, Incident Reporting System, and ticketing

system. Bulletins and Cyber Alerts are transmitted electronically.

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?

Not applicable. No personally identifiable information is shared with external organizations.

5.5 How is the shared information secured by the recipient?

Not applicable. See 5.1 and 5.4.

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

Not applicable. See 5.1 and 5.4.

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

US-CERT only maintains the contact information it may collect within the US-CERT, and does not share it with external or internal organizations. Organizations other than US-CERT are entitled to the bulletins and other information US-CERT releases, but not the personally identifying information of the reporting entity or person. Only US-CERT authorized users can see the personal contact information gathered through the call center, Incident Reporting System, and ticketing system.

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?

Yes. While the collection of contact information is not required to report a cyber-related incident, notice is provided to the regarding the potential uses of the information to the reporting individual prior to their submission of an incident. Further notice is provided by our Privacy Policy available at the following

site http://www.us-cert.gov/privacy.html#privacy.

US-CERT also complies with the "No Disclosure Without Consent Rule" and our website clearly states that the information will not be disclosed without explicit consent from the individual or if the disclosure is required pursuant to 5 U.S.C. §§552a(b)(1) – (12).

This collection of personal information is covered by the DHS System of Records Notice 002 published December 6, 2004 69 Fed Reg 70460 DHS/ALL 002.

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

Individuals have the right to voluntarily provide (or decline to provide) their contact information when submitting information regarding a cyber-related incident or submitting a trouble ticket through the ticketing system. If the submitter chooses to not submit information US-CERT will collect their report and process it as it would any other.

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?

If individuals choose to join a mailing list for one of the US-CERT information products, they may submit an email address, or choose to provide the US-CERT with personal information - like filling out a "Contact Us" form with personal information and submitting it to the US-CERT through the web site; the US-CERT will use that information to send citizens information product(s) requested, or to respond to a message and to help the US-CERT get the information to the party requesting the data.

If individuals choose to submit information regarding a cyber-related incident, they may do so via the 24x7 Incident Reporting System or through our Call Center. 24x7 also serves as a ticketing system. Individuals from the private and public sector may contact US-CERT through 24x7, whereby the individual's contact information and the nature of the concern is collected. If the problem is one that cannot be addressed through 24x7's resources, a trouble ticket is created and notification is sent to the appropriate program within US-CERT for handling.

Similar to the US-CERT mailing lists, the Incident Reporting System, call center, and ticketing system protocol are structured to permit citizens to provide – or not provide – their personal data; if they choose to provide such data, our existing privacy and security policies, as well as the structure of the website and Call Center submissions, outline in great detail notices, choice, access, and consent issues.

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

There was a risk that the individual is unaware of the notice provided. To mitigate this risk, we included statements on each step of the reporting process for the Incident Reporting System and Call Center to ensure that the individual has adequate notice of the collection and the potential uses of the information.

For example, if a report is taken through the phone, the call agent is required to give notice to the person that any information they provide is voluntary, and if they choose to provide information, their information will be used for limited purposes. The reason information can be collected but is not required is that sometimes it is helpful to the researcher assigned to the code or incident to follow up with the original submitter should the information available be incomplete or somehow inaccurate.

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?

By written request, each individual is able to see the exact information that the 24x7/US-CERT holds on them and is entitled to have a copy made of his or her record. Sandy Ford Page, Department of Homeland Security, Preparedness Directorate, Director of Disclosure, 202-282-8522, FOIA.PD@dhs.gov

7.2 What are the procedures for correcting erroneous information?

An individual can submit a written request amendment to amend his or her record. Ten working days after the receipt of the amendment request, US-CERT acknowledges in writing that it has either: (a) corrected any information which the individual asserts is not accurate, relevant, timely, or complete; or (b) informs the individual of our refusal to amend in accordance with the request, the reason for refusal, and the procedures for administrative appeal. If the individual disagrees with our refusal, US-CERT complies with the requirements for review under 5 U.S.C. §§ 552a(c)(4), (d)(3), (d)(4).

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

If the submission is through the Incident Reporting System, the system asks the individual to verify their information prior to the final submission of the data. If the individual contacts the Call Center and speaks to a representative, the representative verifies the individual's contact information prior to ending the telephone call.

7.4 If no redress is provided, are alternatives available?

Not applicable. Redress is provided.

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.

Individuals that choose to provide contact information are given the opportunity, through written request, to see the exact information that 24x7/US-CERT holds on them and is entitled to have a copy made of his or her record (see 7.1, 7.2, and 7.3).

Further, a reporting individual has the right to amend his or her record by submitting a written request amendment. Ten working days after the receipt of the amendment request, US-CERT acknowledges in writing that US-CERT has either: (a) corrected any information which the individual asserts is not accurate, relevant, timely, or complete; or (b) informs the individual of our refusal to amend in accordance with the request, the reason for refusal, and the procedures for administrative appeal. If the individual disagrees with our refusal, US-CERT complies with the requirements for review under 5 U.S.C. §§ 552a(c)(4), (d)(3), (d)(4).

24x7/US-CERT complies with all procedural rights concerning access, correction, and redress as provided for in the Privacy Act of 1974.

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?

24x7/US-CERT provides only those who require access with permission to view the data. The class of users with this access includes security analysts and system administrators.

8.2 Will contractors to DHS have access to the system?

Yes, certain contractors will have access to the system.

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

Yes. Roles and privileges are determined through the use of secure UserIDs and passwords. The UserID and related password allow the system to distinguish user roles and system access.

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

US-CERT determines access principles on a need to know such data for business and security purposes.

From a systems application perspective, administrator management, through regular physical and electronic audits, will ensure: Passwords are not stored in a clear text file; Machines are not configured to automatically log on a particular UserID and password when system is booted; Passwords are changed or expire in 90 days or less; Protocols and settings do not enable a password to be reused for at least 6 iterations and only one user per account is allowed; Never assign a login account a password that is the same string as the UserID or that contains the UserID and never install a guest/guest account; Rename or delete all default passwords provided by the vendor; Deactivate unused accounts monthly. Consider an account unused if no login has occurred in 90 days; The manager or owner of the host shall revalidate all user IDs at least annually; Never set any password equal to the null string, which is equivalent to no password at all. The IT system shall ensure that each user is authenticated before IT system access; Replace passwords whenever a compromise is suspected; Terminate user accounts when a user transfers or has been terminated; and Reset passwords.

For the end user, the password of those persons granted permission to access a system must; Be at least 8 characters in length and must be changed at least every 90 days; Contain a combination of alphabetic, numeric, and special characters and not contain any two identical consecutive characters; Contain no more than three identical consecutive characters in any position from the previous password; Not be identical to any of the previous 6 passwords and not contain any dictionary word in any language; and Passwords shall not contain any proper noun.

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

Preparedness implements and enforces an account lockout policy that limits the number of consecutive failed logon attempts and shall configure systems to lock out a user account after a specified number of failed logon attempts as well as establish and monitor threshold limits for the amount of time a session is inactive before the session timeout feature is invoked.

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

Preparedness ensures audit trails and audit logs are recorded and retained in accordance with the Homeland Security Department Records and Information Management Program.

In addition, auditing and intrusion detection capabilities are provided through firewalls and server logs, which alert the US-CERT intrusion detection team. Proactive scanning and monitoring of logs and events on a daily basis assists in identifying incidents as early as possible to mitigate potential issues. The US-CERT team is operated on a 24x7 basis and coordinates up to escalation support. The support number and email address for the team is displayed on the user's workstation. Audit trail is maintained and stored to facilitate investigation of incidents. US-CERT will examine appropriate identification as well as log review program. Incident reporting policies will include not only the US-CERT but also the Information System Security Manager (ISSM), where appropriate.

US-CERT has conducted a risk assessment of the security controls and reviews the assessment on an on-going basis. US-CERT tests the IT for security vulnerabilities on an on-going basis, including technical,

managerial, and physical security access.

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

Personal information is gathered and maintained in accordance with pertinent Federal rules and regulations, including the Privacy Act of 1974, the E-Government Act of 2002, the Government Paperwork Reduction Act, and other relevant rules and regulations. Questions relating to privacy are forwarded through the Preparedness liaison to the DHS Privacy Office, and training is being conducted to ensure that individuals working with personal information are educated on its proper handling and use. Furthermore, privacy issues are highlighted for all IT projects within the Preparedness Directorate.

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

24X7 has not completed an approved DHS C&A process to date. However, 24X7 began the DHS C&A process in May 2006 and US-CERT expects to complete the review by the end of the first quarter of Fiscal Year 2007.

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

There is the risk that inadvertent access to the data may occur. To mitigate this risk, and in accordance with the DHS Sensitive Systems Handbook, Preparedness ensures effective security controls and authentication. By enforcing system policies and settings and strong passwords, Preparedness protects the privacy of systems which promote or permit public access and the integrity of the data itself. Requirements Identification: Preparedness will include the following policies, practices, guidance, and legal requirements for this process: DHS 4300 - IT Systems Security - Sensitive Systems Pub - Vol I Part A; Federal Information Security Management Act of 2002; OMB Circular A-130 Appendix III, Security of Federal Automated Information Systems; Computer Security Act of 1987; OMB Circular A-11, Preparation and Submission of Budget Estimates; Presidential Decision Memorandum (PDD-63), Critical Infrastructure Protection; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, Security Metrics Guide for Information Technology Systems.

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?

Certain tools within the Program were purchased and installed, however the 24x7 Incident Handling and Response Center capabilities were built from the ground up.

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

Activity and Audits: US-CERT implements and enforces an account lockout policy that limits the number of consecutive failed logon attempts and shall configure systems to lock out a user account after a specified number of failed logon attempts as well as establish and monitor threshold limits for the amount of time a session is inactive before the session timeout feature is invoked. Preparedness ensures audit trails and audit logs are recorded and retained in accordance with the Homeland Security Department Records and Information Management Program.

Access Control and Certification and Accreditation: US-CERT ensures, through the requirements traceability matrix process, access controls be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times. US-CERT ensures remote access and dial-in capabilities provide strong identification and authentication and protect SBU information. US-CERT will certify and accredit systems at initial operating capability and every 3 years thereafter, or whenever a major change occurs, whichever occurs first.

9.3 What design choices were made to enhance privacy?

In accordance with the DHS Sensitive Systems Handbook, Preparedness ensures effective security controls and authentication. By enforcing system policies and settings and strong passwords, Preparedness protects the privacy of systems which promote or permit public access and the integrity of the data itself. Requirements Identification: Preparedness will include the following policies, practices, guidance and legal requirements for this process: DHS 4300 - IT Systems Security - Sensitive Systems Pub - Vol I Part A Federal Information Security Management Act of 2002 OMB Circular A-130 Appendix III, Security of Federal Automated Information Systems Computer Security Act of 1987 OMB Circular A-11, Preparation and Submission of Budget Estimates Presidential Decision Memorandum (PDD-63), Critical Infrastructure Protection National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, Security Metrics Guide for Information Technology Systems System.

With respect to the handling of the personal contact information provided by reporting individuals, US-CERT has instituted controls to ensure that only those who require access are given permission to view the data. Further, US-CERT sanitize data to remove citizen names in the limited instances where such data is provided to ensure the reporting source of the information is not released prior to the distribution of Cyber Security Bulletins or Cyber Alerts.

Conclusion

The primary goal of the 24x7 Incident Handling and Response Center is to act as a communication hub for the US-CERT. The US-CERT is responsible for a tremendous amount of information and communication amongst the Federal government and private sector. Any information that could in any way identify and individual is kept within the US-CERT itself and is not disseminated to any US-CERT subscriber. US-CERT values the public, private, and federal sector contributions that are made to its operations, so it is imperative that US-CERT maintain the privacy of any individual (private or public sector) that submits information regarding a system breach, malicious code, wishes to subscribe to a US-CERT product, or has a simple inquiry. US-CERT has taken the appropriate measures to ensure that such any personally identifying information is collected, maintained, and disposed of in a reasonable and prudent manner.

Responsible Officials

Michael Witt
National Cyber Security Division
Department of Homeland Security
(703) 235-5160

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security