Privacy Impact Assessment

for the

Malware Lab Network

May 4, 2010

Contact Point

Byron Copeland
U.S. Computer Emergency Readiness Team
National Cyber Security Division
National Protection and Programs Directorate
Department of Homeland Security
888-282-0870

Reviewing Official

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
703-235-0780

Abstract

The goal of the Department of Homeland Security (DHS or Department) National Protection and Programs Directorate (NPPD) is to advance the risk-reduction segment of the Department's overall mission. To meet this goal, the NPPD/U.S. Computer Emergency Readiness Team (US-CERT) provides key capabilities in four cyber mission areas: 1) Alert, Warning, and Analysis; 2) Coordination and Collaboration; 3) Response and Assistance; and 4) Protection and Detection. The Malware Lab Network (MLN) contributes critical support to existing tools used by US-CERT to better meet these cyber mission areas. The MLN collects, uses, and maintains analytically relevant information in order to support the Department's cyber security mission, including the prevention and mitigation of cyber attacks, protection of information infrastructure, the assessment of cyber vulnerabilities, and response to cyber incidents. DHS is conducting this PIA to publicly analyze and evaluate the personally identifiable information (PII) within the MLN.

Overview

US-CERT provides response support and defense against cyber attacks for the federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local governments, industry, and international partners. By interacting with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public, US-CERT provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the federal government about cyber security.

US-CERT's MLN is a segregated, closed computer network system, protected by multiple firewalls, used to analyze computer network vulnerabilities and threats. Typically, the MLN receives information about computer security vulnerabilities and threats in the form of the actual malicious code or copies of computer hard drives (images), received by the Department or other federal agency, and the MLN analyzes the code or images in order to discover how to secure or defend computer systems against the threat. The corrective action information is published in US-CERT products such as vulnerability reports or alerts.

The MLN has a website and receives information from the public and/or government agencies for reporting potentially dangerous and/or suspicious cyber information to US-CERT for risk analysis. Information transmitted to US-CERT may include, among other information: malicious codes; computer viruses; worms; spyware; bots; and Trojan horses. In general, any form of an attack tool may be transmitted since they, and the vulnerabilities exploited when an attack occurs, present a real and present danger to the security of domestic information systems. The MLN provides a mechanism by which information regarding cyber threats can be collected and contained in a highly secure environment. A comprehensive evaluation of the threat can thereafter be conducted by expert analysts so as to improve the overall understanding of current or emerging cyber threats. The primary objectives of the MLN are to:

- Develop procedures for the safe and secure handling of malicious attack tools in a manner consistent with best practices;
- Collect potentially or confirmed malicious tools to facilitate threat assessments;
- Provide the capability to deliver immediate actionable information and add additional detail as more facts emerge concerning a cyber incident so to better understand the scope and nature of the attack;
- Enhance analysis efforts by maintaining a robust analysis laboratory that permits more dissection of malicious attack tool information; and

- Produce detailed reports of analysis activity and findings.

To assess risks related to cyber threats the MLN accepts information from a wide variety of sources that may identify potentially dangerous information that poses a risk. For example, the MLN performs analysis of the files it receives from the public and other government sources. Once a suspicious file is identified, it undergoes a deeper technical analysis to make a better determination of the type of threat, and/or any system vulnerabilities. This analysis includes open-source research on computer network security vulnerabilities and threats to provide short and long-term situational awareness and exposes emerging malicious tools that have not been previously identified because they are increasingly subtle and sophisticated. Such deep technical analysis also results in improved response policies and technological guidance being developed and communicated quickly and broadly.

By conducting this analysis, the MLN plays a critical role in improving the security of federal government computer systems as well as enhancing non-federal cyber security. While achieving this goal, the MLN may receive PII when the information is related to a computer network security vulnerability or threat. Additionally, members of the public and/or government agencies voluntarily provide contact information that enables MLN employees to follow up on the reported information when necessary. This PIA is also being conducted to demonstrate the in-depth analysis of identified privacy risks and the mitigation solutions that were implemented to enhance privacy and security of the MLN.

Section 1.0 Characterization of the Information

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 collected, used, disseminated or maintained in the system?

The MLN is used to collect, process, and store a broad range of information voluntarily submitted by members of the public and/or government agencies relating to cyber threats. The information may include PII, Protected Critical Infrastructure Information (PCII), IP addresses, and other information that is analytically relevant to the threat. In addition, contact information from any individual and/or entity submitting information to the MLN is retained, such as names, telephone numbers, and/or e-mail addresses which may be needed to perform follow-up inquiries.

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

The information collected within the MLN comes from a variety of sources, including: individuals, private sector entities, government agencies, and other named or anonymous sources who voluntarily contact US-CERT to report incidents such as cyber threats, vulnerabilities, and suspicious activity.

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

The MLN collects, uses, and maintains analytically relevant information in order to support the Department's cyber security mission, including the prevention and mitigation of cyber attacks, protection of information infrastructure, the assessment of cyber vulnerabilities, and response to incidents. An in-

depth analysis of the collected and processed information related to cyber threats permits the development of mitigation strategies to further enhance the cyber security of US-CERT's mission partners and customers.

1.4 How is the information collected?

The MLN collects information via a number of methods, such as emails and phone calls from individuals, private sector entities, other government agencies, and other named or anonymous sources who wish to report potentially dangerous and/or suspicious information related to potential malicious threats.

1.5 How will the information be checked for accuracy?

Information on computer network vulnerabilities and threats collected by the MLN is checked for accuracy during the in-depth analysis of the information. To ensure the information collected meets a minimum level of accuracy, analysts perform an initial check to determine the suitability of the information. If the information is determined to be appropriate for the MLN to analyze further, US-CERT checks, characterizes, and prioritizes the information in terms of accuracy, threat potential, type of threat, and vulnerability of the targeted infrastructure. If computer network security vulnerability information contains any information similar to PII, this information is NOT to be checked for accuracy as it is only analyzed and processed insofar as it is relevant to the underlying computer network vulnerability. For example, if an exploit is being transmitted to computer networks using an email address of firstname.lastname@dhs.gov it is not important that firstname.lastname@dhs.gov is a real person or email address, the important factor is that it is being used as a threat to computer systems. Any information such as PII that is voluntarily transmitted to the MLN as contact information would likewise not be checked for accuracy, but would only be used to follow up on a reported computer network security threat report.

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

The MLN furthers the Department's network security and critical infrastructure protection responsibilities assigned in the Homeland Security Act of 2002, as amended, the Federal Information Security Management Act, and related authorities. *See* 6 U.S.C. §§ 101 *et seq*. and 44 U.S.C. §§ 3541 *et seq*. The MLN is covered by the DHS/ALL 002 - Mailing and Other Lists System of Records Notice (SORN).

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

In the course of analysis, PII may be encountered. In these situations MLN operates in compliance with internal DHS security and privacy policy and guidance. Also, MLN has integrated robust security policies and procedures into its risk management plans and routinely tests the security of its systems and system components. For example, physical and logical access controls are factored into the risk management. Testing of the systems security controls is performed annually and in accordance with all federal systems security requirements. Situations with privacy implications are addressed with the NPPD National Cyber Security Division (NSCD) Oversight and Compliance Officer; the NPPD Cyber Security and Communications (CS&C) Oversight and Compliance Officer; the NPPD NCSD Information Systems Security Officer; the NPPD Information Security Officer, the NPPD Privacy Officer, and Chief Privacy Officer.

Additionally, the establishment of rules of behavior and best practices such as performing audits, maintaining logs, and abiding by breach notification guidance, protect against misuse of information. In accordance with internal DHS policy outlined in the Sensitive Systems Handbook, appropriate security controls and certifications were completed before the MLN was operational. Other privacy and security measures in place include annual review of security controls, rigorous testing of security controls, and limited access to the MLN and data collected, processed or stored by the MLN to authorized users with a need to know. The MLN complies with all applicable requirements.

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 MLN collects, uses, and maintains analytically relevant information in order to support the Department's cyber security mission, including the prevention and mitigation of cyber attacks, protection of infrastructure information, the assessment of cyber vulnerabilities, and response to cyber incidents. An in-depth analysis of the collected and processed information related to the cyber threats permits the development strategies to further enhance the cyber security of US-CERT's mission partners and customers. The information is disseminated as US-CERT products in the form of Situational Awareness Reports (SAR), Federal Information Notices (FIN), Critical Infrastructure Information Notices (CIIN), Early Warning Information Notice (EWIN), Malware Initial Findings Report (MIFR), Malware Analysis Report (MAR) and GFIRST Alerts via the GFIRST Portal.

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

The MLN uses tools that are commercially available industry standard malware reverse engineering and analysis tools in order to produce reports of malware analysis activity and findings.

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

Commercial and publicly available information on computer network security vulnerabilities and threats are used by the MLN to conduct analysis to further identify the current cyber threat and the tools, techniques, and tactics used.

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.

To ensure that information is handled in accordance with appropriately defined and authorized uses, the MLN adheres to privacy and security safeguards and controls, also described in section 1.7. The NPPD US-CERT Oversight and Compliance Officer; NPPD CS&C Oversight and Compliance Officer; the

NPPD Privacy Officer; Chief Privacy Officer; and the IG, all may exercise their oversight responsibilities to ensure that information is properly protected in accordance with applicable laws, regulations, and policies.

Section 3.0 Retention

3.1 What information is retained?

Information relevant to potential cyber threats and vulnerabilities is retained. This information may include all of the information submitted to the MLN as well as reports generated from the analysis. Information received from the public, private sector entities, other government agencies, or other sources is retained in accordance with DHS and US-CERT procedures.

3.2 How long is information retained?

An approval request is in process. The Department is currently working with the Office of Records Management to develop a disposition schedule that will allow MLN information to be retained for seven (7) years, which will be sent to the National Archives and Records Administration (NARA) for approval.

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

An approval request is in process. The Department is currently working with the Office of Records Management to develop a disposition schedule that will allow MLN information to be retained for seven (7) years, which will be sent to NARA for approval.

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

Ensuring that information is retained for only the minimum amount of time necessary reduces the risks associated with maintaining information. Additionally, all information collected, processed, and stored by the MLN is analyzed to determine appropriateness of further analysis and retention. All captured information resides upon a secured system with appropriate audit logging. The policy of data minimization, a secured system, and auditing mitigates associated risks.

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

The MLN information derived from analysis is shared internally with the US-CERT branches in the form of Malware Initial Findings Reports. The MLN information is also shared with US-CERT leadership for situational awareness.

4.2 How is the information transmitted or disclosed?

The MLN analysis and research is placed into US-CERT reports that are transmitted internally via email using a secured Unclassified/FOUO portal requiring two factor authentication.

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.

In the course of conducting research related to potential cyber threats, or performing analysis or data or information submitted to MLN, PII may be encountered. Although the focus of analysis is only to better identify and understand cyber threats, there exists the possibility that PII may be shared, if determined to be relevant and necessary. In these situations any PII shared is minimized to the extent possible and is only that which is necessary for understanding the underlying computer network security vulnerability. To mitigate the risk of inappropriate internal sharing of PII, US-CERT employees must complete comprehensive privacy training to ensure they are fully aware of the appropriate uses of information. Additionally, US-CERT has well-established and comprehensive information handling processes to enhance personal information security and eliminate possibilities for misuse or abuse. The MLN adheres to all of these internal information security policies, as well as those outlined in DHS and US-CERT information technology security documents.

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

The goal of the MLN is to support US-CERT's capability to enhance situational awareness by creating a better understanding of current cyber threats and ensure that important cyber security information is shared in the most timely and efficient manner possible. The MLN provides its computer security vulnerability analysis to US-CERT that in turn shares information with participating agencies or the private sector in furtherance of the DHS cyber security mission and in accordance with US-CERT policies and procedures. Law enforcement, intelligence, or other agencies with cyber-related responsibilities may be notified when collected information falls under their responsibility.

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?

Sharing PII outside the Department is consistent with the original information collection. The MLN is covered by the DHS/ALL 002 - Mailing and Other Lists SORN. Computer security information, which may contain PII, is shared with the federal agencies that requested the analysis since the information was originally collected by them. PII is not shared outside the MLN unless it is necessary for forming an understanding of the underlying potential cyber threat or vulnerability. The MLN only shares information with participating government agencies and/or the public in furtherance of the DHS cyber security mission and in accordance with established policies and procedures.

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

Publications that may contain MLN information are shared via access to a secure US-CERT website. Otherwise, MLN information that contains PII may be removed from, or accessed from, outside the Department only when strict security measures that safeguard its transmission are in place, including two-factor authentication.

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

The MLN information contained in Cyber Security Bulletins, Cyber Alerts, and other US-CERT publications are generally devoid of PII. In the event that there is an appropriate need to externally share MLN information that contains PII, it would be done only in strict accordance with US-CERT policies and procedures and following security measures that safeguard its transmission such as two-factor authentication.

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?

Notice is provided by the DHS/ALL 002 - Mailing and Other Lists SORN, the publication of this PIA, and the posting of a privacy notice on the web portal that is used to transmit an electronic mail message to the MLN. Information gathered as a result of open-source research is information in the public domain subject to discovery and no notice is required.

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

PII may be required to process or respond to submissions made to the MLN via its web portal, but it is not mandatory that an individual provide this information. A privacy notice is posted on the web portal used to transmit electronic mail messages to the MLN so computer users are aware that they are voluntarily providing some information to the government when they communicate with the government via the Internet, such as when a sender voluntarily includes the information as part of an electronic mail message on the MLN web portal.

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

The privacy notice on the web portal that individuals use to transmit an electronic mail message to the MLN informs senders regarding the authority for the collection of the requested information, the principal purposes of information, that disclosure is not mandatory, how the information provided is used, and who it is made available to, and that by transmitting information the sender is agreeing to disclosure. Information is provided voluntarily without the expectation of a right to limit the use of the information, consistent with all disclosed purposes and uses.

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.

Notice is provided through the DHS/ALL 002 - Mailing and Other Lists SORN, privacy notice on information collection portal and the posting of this PIA. In addition, PIAs regarding the other US-CERT programs are also posted www.dhs.gov/privacy.

Section 7.0 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 that allow individuals to gain access to their information?

As discussed in section 6.1, cyber threat and vulnerability information is not maintained or retrieved based on information that identifies an individual. In the rare cases the MLN collects information that could identify an individual, such as an unspoofed email address within header information or other PII within records incidentally collected as part of a security incident, the information is maintained and indexed by the security vulnerability, not by PII. Any PII submitted to the MLN as contact information is used solely for the purposes of following-up on the submission.

Individuals may request other information about the MLN under Freedom of Information Act (5 U.S.C. § 552) by contacting the DHS FOIA office at:

FOIA Office
U.S. Department of Homeland Security
245 Murray Drive SW
Washington, D.C. 20528-0550
Email: foia@dhs.gov

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

Individuals may request to correct inaccurate or erroneous information by contacting the NPPD Privacy Officer at:

NPPD Privacy Officer
U.S. Department of Homeland Security
245 Murray Drive, SW
Washington, D.C. 20598-0675
NPPDprivacy@dhs.gov

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

Individuals are advised of the procedures for correcting their information through DHS/ALL 002 - Mailing and Other Lists SORN, via the DHS public-facing website (http://www.dhs.gov/index.shtm) or by contacting the NPPD Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW, Washington, DC 20598-0675, or NPPDprivacy@dhs.gov.

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

Formal redress is provided. Individuals may contact the NPPD Privacy Officer at:

NPPD Privacy Officer
U.S. Department of Homeland Security
245 Murray Drive, SW
Washington, D.C. 20598-0675
NPPDprivacy@dhs.gov

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

The MLN provides individuals with all procedural rights concerning access, correction, and redress. In addition, if an individual is dissatisfied with the response to his or her redress inquiry, he or she may appeal to the Chief Privacy Officer, who reviews the appeal and provides final adjudication concerning the

matter. The Chief Privacy Officer may be contacted at Chief Privacy Officer, Attn: MLN Appeal, Department of Homeland Security, Washington, D.C. 20528; or by fax: 1-202-772-5036.

Section 8.0 Technical Access and Security

The following questions 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?

Documented procedures determine which users may access the MLN information. Access to information is strictly limited to authorized personnel only with a need to know for official duties. An administrator is responsible for granting access to registered users and for maintaining and updating a comprehensive list of registered users. Additionally, DHS policy requires a unique user account before access to the DHS network is authorized and a signed user access agreement with a supervisor certification that access is needed for official duties. User access agreements also include rules of behavior regarding responsibilities for safeguarding PII and the consequences and accountability for violating these responsibilities. Completed user access agreements are reviewed and approved by an NPPD Information System Security Officer, who reviews and approves completed user access agreements before unique user accounts are assigned.

8.2 Will Department contractors have access to the system?

Access to the MLN information is given to authorized DHS contractors with security clearances and a justified need to know in conjunction with their contractual duties.

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

DHS provides comprehensive privacy training to all DHS personnel prior to assigning access to the DHS unclassified network. Additionally, personnel with access to the MLN information are given role-specific privacy training and annual privacy refresher training to retain system access.

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

Certification and accreditation for the MLN was completed in early 2010.

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

Robust auditing measures and technical safeguards are in place to prevent misuse of the MLN information. First, DHS has well-established and comprehensive processes that enhance information security and minimize possibilities for misuse or abuse. The MLN adheres to all internal information security policies in accordance with the DHS Records and Information Management Programs. In addition,

the MLN is safeguarded by auditing and intrusion detection capabilities provided through an Intrusion Detection and Protection system, as well as firewalls and server logs which alert an intrusion detection team. To mitigate potential issues, there is daily proactive scanning and monitoring of logs and events to identify incidents as early as possible on a 24x7 basis. Audit trails are maintained and stored to facilitate investigation of incidents. DHS Incident Reporting Guidelines are established and require the involvement of the NPPD Information System Security Officer, when appropriate. Annually scheduled risk assessments are performed on the security controls for security vulnerabilities, including technical, managerial, and physical security access.

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?

To address the privacy risks associated with the sensitivity and scope of the MLN information, a variety of security controls have been implemented. The information is protected by strict administrative, technical, and physical safeguards appropriate to the sensitivity of the information. The MLN operates in accordance with required DHS and federal information security requirements and policies to ensure that information is appropriately safeguarded, and complies with any other applicable business and security requirements defined in the technical environment of US-CERT.

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 What type of project is the program or system?

The MLN is a computer network laboratory environment where US-CERT can receive files and emails regarding malware from the public and other government agencies. It is a secured network environment where MLN administrators can safely receive and prepare files suspected of containing malware for analysis and generate reports from the analysis and findings.

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

The MLN is in the early stage of development. A controlled and limited pilot was previously completed and, based on an analysis of that pilot; the MLN is implementing the systematic solution described in this PIA. If the MLN undergoes any significant modification, or begins to expand its scope, another comprehensive PIA will be conducted and posted.

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

In addition to employing existing technology, systems, processes, and facilities, the MLN employs foundational hardware and software to support a domain name and electronic mail addresses to be used by the public and/or government agencies for submitting potentially dangerous and/or suspicious cyber information to US-CERT for analysis.

Responsible Official

Byron Copeland, Chief, Digital Analytics Branch
United States Computer Emergency Readiness Team
National Cyber Security Division
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security