Privacy Impact Assessment
for the

U.S. Secret Service Cyber Awareness Program (Cyveillance)

DHS/USSS/PIA-011

December 14, 2012

Contact Point
Latita M. Payne
Privacy Officer
United States Secret Service
(202) 406-5838

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (Secret Service) has procured under contract the Cyveillance system as part of its Cyber Awareness Program. Cyveillance searches for information regarding the Secret Service and investigatory and protective intelligence information. The Secret Service is conducting this Privacy Impact Assessment (PIA) because, while the primary purpose of Cyveillance is not to collect personally identifiable information (PII), the content of interest to the Secret Service that is collected by Cyveillance may contain PII.

Overview

Cyveillance, a subsidiary of QinetiQ of North America, is under contract by the Secret Service to search available information related to the Secret Service and its missions.

The information captured by Cyveillance is reviewed by Cyveillance personnel to identify the results that appear to fall within the parameters of the Secret Service's stated requirements. Potentially relevant information related to the Agency's missions is forwarded to Secret Service personnel who determine whether further investigation is required to assess the content (e.g., to determine if it is a viable or potentially viable threat). If further investigation is deemed necessary, the information obtained through Cyveillance is incorporated into the Protective Research Information Management System (PRISM-ID)[1], an existing Secret Service system. Content that relates to the Secret Service brand (i.e., mention of the Secret Service name) is forwarded to Secret Service personnel for informational purposes only; following its review, this information is deleted and is not retained by the Agency.

The Secret Service shares information in its possession, regardless of origin, with those individuals or agencies with a need-to-know in order to facilitate the detection and/or prevention of crime, or to provide for the protection of individuals, events, and facilities. This sharing is in accordance with the routine uses outlined in the applicable System of Records Notices: information related to protective intelligence is covered by the DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011),[1] and information related to criminal investigations is covered by DHS/USSS-001 Criminal Investigation System of Records, 76 FR 49497 (August 10, 2011).[2]

The privacy impact on individuals is limited since the primary purpose of Cyveillance is not to collect PII. The Secret Service retains only that information derived from Cyveillance that

[1] See DHS/USSS/PIA-003 Protective Research Information Management System (PRISM-ID) http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-usss-prism-id.pdf
[1] http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm
[2] http://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm

is required for investigations in furtherance of the Secret Service's missions. Retained information is indexed in a separate system (PRISM-ID).

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The collection of this information is authorized by the Secret Service's statutory authority, 18 U.S.C. §§ 3056 and 3056A, Powers, Authorities, and Duties of United States Secret Service.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Information identified by Cyveillance that is not retained for further investigation is not stored in a system of records, and because it is not retrieved by personal identifier, there is therefore, no applicable SORN. To the extent that any information identified by Cyveillance as related to protective intelligence is ultimately incorporated into an Agency system of records, that information is covered by DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011). Similarly, to the extent that information related to criminal investigations may be incorporated into a system of records, it would be covered by DHS/USSS-001 Criminal Investigation System of Records, 76 FR 49497 (August 10, 2011).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The Secret Service is currently engaged in efforts to document Cyveillance's security plan.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Cyveillance outputs are temporary records and are immediately discarded when they are no longer needed for agency business in accordance with the applicable disposition schedule. To the extent that Cyveillance outputs are incorporated into an Agency system of records, such information would be covered by the retention schedule applicable to that record type, for example, protective intelligence records and criminal investigative records.[3]

[3] See retention schedule for DHS/USSS-004 at: http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm and DHS/USSS-001 at: http://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Cyveillance outputs are not covered by the PRA.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Cyveillance identifies content that falls within the search parameters dictated by the Agency. While the general purpose of Cyveillance is not to collect PII, the collected information may contain PII. As Cyveillance's function is not to collect PII, it is not possible for the Secret Service to know what PII, if any, may be contained in the collected information.

Potentially relevant information, which is forwarded to the Secret Service via Agency email for review is either not used and deleted by the Secret Service following review or determined to potentially implicate the missions of the Agency and forwarded to the appropriate Agency officials for possible further action. If further investigation is deemed necessary, the Agency initiates an investigation and incorporates the information into PRISM-ID. As part of such an investigation, the information collected by Cyveillance that prompted the investigation may be disseminated via Secret Service email to other Secret Service entities.

2.2 What are the sources of the information and how is the information collected for the project?

Cyveillance uses technology to identify information related to the Secret Service and its missions in accordance with parameters established by the Agency.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of data searched and identified by Cyveillance is only addressed if the Agency takes action based upon the information identified by Cyveillance; the Cyveillance program itself does not address and is not concerned with data accuracy.

If the Agency determines that the information identified by Cyveillance warrants further investigation or response by the Agency, trained personnel take appropriate action. When PII collected by Cyveillance is relevant to an investigation, the accuracy of the PII is determined as part of the Agency's subsequent investigation.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Cyveillance could collect PII that does not have an inherent tie to the Secret Service or its missions.

Mitigation: Cyveillance collects information using carefully defined parameters, specifically tailored to identify relevant information for official purposes, while also minimizing false positives (*i.e.*, mis-hits or information unrelated to the Secret Service's missions). All information collected at the direction of the Secret Service that is not needed to carry out the Agency's missions is discarded.

Privacy Risk: Cyveillance search terms could be too broad or include requests for PII.

Mitigation: The search terms are continuously evolving to more effectively and efficiently meet the Secret Service's protective intelligence goals and processes in addition to being tailored to particular events and external circumstances. The Secret Service's legal counsel reviews terms used for some specific events and has engaged in numerous discussions with relevant individuals regarding scope and internal policy as well as received guidance from the Department of Justice. Finally, the individuals who provide the parameters for the search terms are experienced and trained in the proper collection and use of PII.

Privacy Risk: Cyveillance might collect information that describes how individuals exercise their First Amendment rights.

Mitigation: The search parameters established by the Secret Service are not intended to collect information describing the exercise of individuals' First Amendment rights, nor is it Cyveillance's function to collect any PII. To the extent Cyveillance collects such information it must be relevant to an authorized Secret Service law enforcement activity and, as such, permitted by the Privacy Act. To the extent such information is not relevant to a Secret Service law enforcement activity, it is deleted as noted above.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

Cyveillance uses information to identify content concerning the Secret Service and its missions that may necessitate a response from the Agency. Cyveillance outputs that are determined to contain credible information related to the Secret Service's protective and/or investigative responsibilities may be used to initiate or further investigations.

Cyveillance outputs regarding mention of the Secret Service name are reviewed for informational purposes only and are then discarded.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. The Secret Service does not use Cyveillance to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. There are no other components with assigned roles and responsibilities related to Cyveillance.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Cyveillance will collect and report incorrect PII that may be used in an investigation.

Mitigation 1: The information collected and reported by Cyveillance is limited to that which individuals have elected to self-report.

Mitigation 2: In the event of an investigation, Secret Service personnel, who have received specialized training in investigative and analytical techniques, review all pertinent information and conduct research to verify the information, including the accuracy of the collected PII, in order to further the Secret Service's missions.

Privacy Risk: PII collected by Cyveillance may be used by Agency personnel for an improper and/or unauthorized purpose.

Mitigation: Access to the information identified by Cyveillance that is forwarded to the Secret Service is limited to those Agency employees who have an official need to access it and

are trained in its proper use of such information, as well as on the proper use of PII. Access to the information contained within Cyveillance itself is limited to a specific number of contractors and is controlled by the system's secure IT infrastructure, which requires login, logs activity, and uses firewalls, as well as other computer security measures.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

DHS/USSS-004 Protection Information Systems System of Records, 76 FR 6940 (October 28, 2011), and DHS/USS-01 Criminal Investigation System of Records, 76 FR 49497 (August 10, 2011), provide general notice regarding the collection of information and the routine uses associated with the collection of the information, that Cyveillance follows. This PIA also serves as public notice of the existence of Cyveillance in support of the Secret Service missions.

Advance notice of the collection of information found in online content is often not possible because the true identity of the author is unknown to the Secret Service and/or it could compromise ongoing law enforcement investigations or otherwise impede law enforcement proceedings.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The purpose of Cyveillance is to identify information regarding the Agency and its statutory missions. To the extent that individuals do not want their information available, they may elect to remove it, or request the original poster to remove it.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be aware of the existence of Cyveillance and the data its collects and reports to the Secret Service.

Mitigation: This PIA serves as public notice of the existence of Cyveillance in support of the Secret Service missions. The routine uses of information of the type collected by Cyveillance are described in DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011), and DHS/USSS-01 Criminal Investigation System of Records, 76 FR 49497 (August 10, 2011).

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

All information collected by Cyveillance in support of the Secret Service that does not warrant further investigation is deleted from Cyveillance not later than ten business days from its collection, and is also deleted from Secret Service systems and email accounts. To the extent information generated by Cyveillance warrants further action by the Agency, the information becomes a part of the Agency's record of the actions taken and will be retained for the specific time period specified in the applicable records retention schedule. (See DHS/USSS/PIA-003 Protective Research Information Management System (PRISM-ID)).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Information may be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: All information collected by Cyveillance in support of the Secret Service that does not warrant further Agency action is destroyed. Information collected by Cyveillance which warrants further Agency action becomes a part of a system of records and retained for a proscribed period of time in accordance with the appropriate established records retention schedules.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information collected and reported to the Secret Service by Cyveillance is not automatically shared with external entities as part of normal Agency operations. When such information warrants further Agency action, the information may subsequently be disclosed to external entities that need it in furtherance of their lawful purposes and/or the Secret Service's lawful purposes. Identified information that becomes part of an investigative or criminal case file may be shared on a need-to-know basis with federal, state, and local law enforcement agencies, other foreign and domestic government units, or private entities in accordance with the routine uses outlined in the applicable SORN.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing of information which is collected and reported by Cyveillance and is incorporated into an Agency system of records may be disclosed in accordance with the routine uses outlined in the applicable SORNs. Routine uses in DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011) and DHS/USSS-01 Criminal Investigation System of Records, 76 FR 49497 (August 10, 2011) specifically authorize the disclosure of information on a need-to-know basis to federal, state, and local law enforcement agencies, other foreign and domestic government units, or private entities.

6.3 Does the project place limitations on re-dissemination?

There are no limits on re-dissemination. It is presumed that re-dissemination by authorized recipients may be necessary to further criminal investigations or to support protective operations.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The only Cyveillance outputs currently retained by the Secret Service are those that are required for investigations in furtherance of the Secret Service's missions. This retained information is indexed in a separate system, PRISM-ID. Case files created within PRISM-ID record the recipient of any information that is subsequently shared outside the Secret Service.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information originally collected and reported by Cyveillance to the Secret Service will subsequently be disclosed to unauthorized individuals.

Mitigation: All Secret Service employees, including those individuals with access to the information collected and reported by Cyveillance, receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. Disclosures must be documented and case files created within PRISM-ID record the recipient of any information that is subsequently shared outside the Secret Service.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

To the extent information generated by Cyveillance warrants further action by the Agency and becomes a part of the Agency's record of the actions taken, the procedures for access are stated in the SORNs for the applicable systems of records: DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011); and DHS/USSS-01 Criminal Investigation System of Records, 76 FR 49497 (August 10, 2011). As law enforcement systems, the Protection Information and the Criminal Investigation Systems of Records are exempted from the Privacy Act's notification, access, and amendment provisions to prevent harm to law enforcement investigations or interests. However, access requests will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA Officer, Communications Center (FOI/PA), 245 Murray Lane, Building T-5, Washington, D. C. 20223, as specified in the applicable SORNs.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures are the same as those outlined in Section 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

The procedures for requesting the correction of information are specified in the applicable SORNs and on the Secret Service's public webpage. (http://www.secretservice.gov/foia.shtml)

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: An individual may have limited access or ability to correct their information.

Mitigation: To the extent this information Cyveillance collects and reports is self-reported, individuals can correct the information as it appears before it may be entered into an Agency system of records. Additionally, the information collected and reported by Cyveillance is deleted from Cyveillance not more than ten business days after collection. Individuals may request access to information about them under the FOIA and Privacy Act and may also request their information be corrected.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Cyveillance activity is directed by the Secret Service. Information collected and reported by Cyveillance to the Secret Service is reviewed by Secret Service personnel to ensure its relevance to the Secret Service missions. That information which is not relevant is purged by Cyveillance and the Secret Service. Secret Service personnel who review the information are trained on the proper and authorized uses of the information obtained from Cyveillance, as documented in this PIA.

Cyveillance routinely undergoes self-audits to ensure that existing privacy protections and security protocols are being followed.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All Secret Service employees are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. DHS has published the "Handbook for Safeguarding Sensitive PII," providing employees and contractors additional guidance. Cyveillance personnel receive privacy training concerning appropriate uses of information from parent company QinetiQ.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

DHS physical and information security policies dictate who may access Secret Service computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to Secret Service computers. Access to the information collected and reported by Cyveillance is strictly limited by access controls to those who require it for completion of their official duties. Cyveillance uses a secure information technology (IT) infrastructure to support the Secret Service that requires login, audits activity, and uses firewalls and other computer security measures. Cyveillance IT infrastructure is housed within a secure facility protected by various physical security apparatus such as alarms, door locks, and controlled access.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

There are no existing or planned information sharing agreements for information collected or reported by Cyveillance. If information sharing agreements are contemplated in the future, program managers will review proposed agreements to ensure proposed information disclosures are authorized under a category of routine use or other relevant authority.

Responsible Official

Richard K. Elias, Assistant Director
Office of Strategic Intelligence and Information
United States Secret Service
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security