Privacy Impact Assessment

for the

eForce (formerly known as Use of Force) Reporting Application System)

DHS Reference No. DHS/USSS/PIA-032

July 24, 2024

Homeland Security

Abstract

The United States Secret Service (USSS or Secret Service) Use of Force reporting application system, hereafter called eForce, allows USSS law enforcement personnel to input incident data when an agency officer or agent uses any level of force beyond compliant handcuffing, verbal commands, or de-escalation techniques. The system also maintains data on certain incidents in which force is not used against a person (e.g., a Taser is drawn from its holster, but it is not used). eForce makes it possible for the Secret Service Office of Strategic Planning and Policy/Enterprise Analytics Division to compile use of force data and report and share it within the agency, as appropriate, with the Department of Homeland Security (DHS), and, consistent with Section 6 of Executive Order 14074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety," with the Federal Bureau of Investigation (FBI). The Secret Service is conducting this Privacy Impact Assessment (PIA) because eForce maintains personally identifiable information about individuals and Secret Service employees involved in reportable use of force incidents.

Overview

As part of its mission to protect leaders and safeguard the U.S. financial infrastructure, the Secret Service statutorily performs law enforcement operations during which incidents may occur that require the use of force by law enforcement personnel. eForce is used by the Secret Service to document all incidents in which force is utilized.

eForce was developed by the USSS Agency Software Solutions team and is secured within the Application Provisioning System. The Application Provisioning System is a tiered system that maintains, transmits, and processes data, and facilitates team sites, collaborative workspaces, and special applications that design, develop, deploy, and sustain software solutions. It provides mission and business information technology solutions in a completely centralized, secure, and redundant environment. Applications are developed and configured to ensure that the services provided are collaborative and facilitate the desired information management solution for the Secret Service business or data owner. Application Provisioning System data is encrypted using methodologies used for databases as governed by Secret Service, DHS, and federal information technology system policies.

The Secret Service Office of Strategic Planning and Policy is responsible for oversight of eForce. The Office of Strategic Planning and Policy/Enterprise Analytics Division will compile and disseminate aggregate data within DHS and to the FBI, and is responsible for records retention management within eForce.

All Secret Service law enforcement personnel will have access to eForce to enter reportable incidents. Law enforcement supervisors have access to review and approve (i.e., to ensure the

report is properly completed) reportable incidents created by their subordinates; they cannot change the information entered by their subordinates. Designated employees assigned to the Office of the Chief Counsel and the James J. Rowley Training Center Use of Force Branch will have access to review incident reports; they also cannot modify or change the information entered by the reporting officer/agent.

eForce maintains information about reportable incidents related to use of force, including certain incidents when force is not used (e.g., a Taser is drawn from its holster, but is not used). Limited personally identifiable information will be collected on the individual against whom force was used and the agents and officers who used force. The types of information collected include first and last name, age, date of birth, gender, race, height, weight, whether the person was taken into custody, and whether they were injured during the incident. If a person is deemed a subject ("subject" in this context is defined as the person against whom force was used, or at whom force was directed), the following additional information is collected: details of their arrest if they were arrested, whether the subject is a juvenile, their mental health state (based on the officer's/agent's observations)[1], the primary charge, if their information is located within the Criminal Justice Information Services Criminal Case Number (CJIS/CCN) system, if an SSF 4483, *Prisoner Medical Clearance Form*, was completed, if emergency medical service was called, and whether the subject was taken to the hospital. If a Taser was deployed, specific information related to the Taser is collected. There is also a narrative space in which the officer/agent must provide further details about the incident. Each completed incident will be assigned a unique number. The incident may be retrieved by using the unique identifier assigned to each incident or by searching for the officer's name and incident date.

Subsequently, USSS use of force data is reported monthly to the FBI and quarterly to DHS. The USSS Office of Strategic Planning and Policy maintains overall responsibility for eForce, and will access the system to retrieve data in compliance with Executive Order 14074 and DHS policy. Enterprise Analytics Division personnel will access the system to retrieve and share relevant data only (as discussed above). The data shared outside the agency is statistical and solely utilized for the purposes required under DHS policy and Executive Order 14074; therefore, no personally identifiable information maintained in eForce will be shared with DHS and/or the FBI. After the Enterprise Analytics Division retrieves the required data from the system, an employee in the Division will transmit the information to the FBI and DHS.

Within the Application Provisioning System (within which eForce sits), the Application Services team provides archival services, and annually the archives are assessed to ensure only the

[1] Information about the mental health state of an individual is only collected if mental health is the basis for custody. Specifically, if an individual is placed in custody due to a perceived mental health issue that the officer assessed was creating a danger to the individual or others, then this information is reflected in eForce as a reportable incident.

appropriate data is maintained and retained in accordance with the appropriate retention schedule. The data will be retained according to the retention requirements provided in the eForce Records Retention Guidelines and outlined in Section 5 below.

Potential risks to privacy may be associated with eForce users' access or misuse of information. To minimize these risks, eForce has a security module that limits a user access based on access role, area of responsibility, and involvement in an incident. Access to the security module is controlled by the Secret Service Office of the Chief Information Officer and system access roles beyond default for Office of Strategic Planning and Policy employees are granted for reporting and analytical purposes only as needed. The system database also uses an audit log that tracks changes made to incident reports, including who made the changes, the nature of the changes, and a time-stamped snapshot of the incident report following each session of changes. Reports containing data from the system are provided in standard formats and are denoted with "Controlled Unclassified Information" or other applicable marking.

The USSS Office of Strategic Planning and Policy will not routinely share personally identifiable information or incident specific information maintained in eForce outside of the Secret Service or with other government components or outside entities as part of normal operations.

The system will maintain information about incidents in which agents and officers use a specified level of force as defined in Secret Service eForce policy. Limited personally identifying information will be collected on the subject against whom force was used (or directed) and the agents and officers who used force. An officer or agent will document the following types of force, as defined in Secret Service eForce policy:

1. the officer or agent uses more force than is typically used when handcuffing or controlling a compliant subject;
2. a less-lethal[2] device is deployed or used against a subject;
3. an officer or agent discharges a firearm at a person or vehicle; or
4. any person is killed, injured, or complains of being injured following an incident with USSS.

Data will only be input into eForce via a computer-based application that is not available on a mobile device. Upon completion of an eForce report, there are several review steps prior to the form being finalized.

Data retrieval in eForce is by a unique identifier assigned to each incident, an officer's name, or incident date. Only end-users, reviewers, and administrators with special access

[2] "Less-lethal" means any device or technique that is neither designed nor intended to cause death or serious bodily injury. It is also commonly referred to as "less-than-lethal" or "intermediate weapon."

privileges are granted access to the information in eForce. Secret Service systems are accessed through credential authentication. Secret Service personnel are granted role-specific permissions to access eForce based on need-to-know.

If an employee separates from employment with the agency, all access to agency systems is revoked. If an employee is suspected of misusing data maintained in this system, as with any other system, an appropriate inquiry or investigation will be undertaken to determine potential misuse and any appropriate action against the employee. Additionally, access is revoked when an individual no longer serves in the designated role or no longer has a "need-to-know."

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 Secret Service is authorized to collect information maintained in eForce pursuant to 18 U.S.C. §§ 3056 and 3056A. Further, Executive Order 14074 mandates that federal law enforcement agencies collect use of force data in certain circumstances and report that data to the FBI.

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

eForce maintains data entered by Secret Service law enforcement personnel and is used only for reporting and analytical purposes. The Secret Service maintains records related to its protective functions in accordance with the DHS/USSS-004 Protection Information System System of Records Notice.[3] This System of Records Notice governs reports about an individual compiled at various stages through the enforcement of certain criminal laws in conjunction with the execution of the Secret Service's protective mission. Further, the DHS/USSS-001 Criminal Investigation Information System of Records Notice provides notice regarding the collection of subject information in conjunction with the agency's investigative mission.[4]

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

The Application Provisioning System has undergone the Security Authorization process in accordance with DHS and Secret Service policy, which complies with federal statutes, policies, and guidelines. The system's Authority to Operate was renewed on February 22, 2023.

1.4 Does a records retention schedule approved by the National

[3] *See* DHS/USSS-004 Protection Information, 85 FR 64519 (October 13, 2020).
[4] *See* DHS/USSS-001 Criminal Investigation Information, 85 FR 64523 (October 13, 2020).

Archives and Records Administration (NARA) exist?

eForce records managed by the Secret Service meet the definition of "Significant Statistical Program Files" under NARA-approved retention schedule N1-087-11-005.[5]

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.

Due to the law enforcement nature of this information collection, all information maintained within eForce is not covered by the Paperwork Reduction Act.[6]

Section 2.0 Characterization of the Information

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

eForce collects and uses personally identifiable information about Secret Service employees who used force and subjects against whom force was used (or directed). A detailed description of personally identifiable information and other information collected is presented below.

Information about the Secret Service Officer/Agent who used force and completes the form:

- Name (first, middle, last)
- Age
- Gender
- Rank
- Years with Secret Service

Other information collected regarding employees related to their involvement in the incident, specifically:

- Role
- Whether they used force
- Whether they were readily identifiable (i.e., was the officer/agent in uniform or

[5] *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-11-005_sf115.pdf.
[6] 44 U.S.C. § 3501.

clearly identified as law enforcement personnel)

- Did they render aid to subject
- Status (on or off duty)
- Injured
- Emergency medical service
- Hospital

Information on other employees who used force during incident:

- Name
- Role
- Used force
- Attire
- Assignment
- Rank
- Years with Secret Service
- Employment

Information about Subject against whom force was used:

- Name
- Age
- Date of birth
- Gender
- Race
- Height
- Weight
- Custody (i.e., to which facility they were transported (e.g., Arrested, Juvenile, and/or Mental Health))
- Primary charge
- Criminal Justice Information Services Criminal Case Number
- Injured (or injury complaint)

- SSF 4483, *Prisoner Medical Clearance Form*, was completed
- Emergency medical service
- Hospital

Additional Subject Information:

- Subject's mental/criminal history
- Impairment as assessed by the officer (e.g., drugs/alcohol)
- Threats made
- Resistance displayed
- Type of weapon displayed
- Type of weapon used
- Type of force used
- Narrative section

The remaining information collected in eForce related to the incident includes the following:

- Date of incident
- Type of incident
- Criminal Justice Information Services Criminal Case Number or other Case Number
- Type of contact
- Nature of call
- Offense category
- Offenses
- Location
- Environment (e.g., indoors, outdoors)
- Threat(s) made
- Injury sustained or injury compliant, if any

Information will be collected on law enforcement agents/officers who document a reportable incident (as defined in Secret Service eForce policy), and anyone subject to the agent's/officer's use of force. A new report will be created to document each incident, including the agents/officers involved, and any subjects against whom force was used by Secret Service law enforcement

personnel.

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

Information will be collected and manually entered into eForce by the agent/officer involved in a reportable use of force incident. The information entered regarding the subject may be based on responses to questions the agent/officer asked the subject and/or examination of a driver's license or ID card, and compared against any reports written to document the incident to ensure accurate reporting of the subject's information.

Further, the Secret Service ePerson system[7] interfaces with eForce. When an agent/officer enters incident information into eForce, they will include their name and the name of any other agents/officers who used force during the incident. The initiating officer/agent will select Secret Service personnel profiles in ePerson to be added to the eForce incident, rather than manually entering the other agents'/officers' information; this helps to ensure accurate employee data is maintained in eForce.

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

No, eForce does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Information entered into the system by an agent/officer is reviewed by first- and second-line supervisors, members of the Office of the Chief Counsel Legal Training Section, and certain members of the James J. Rowley Training Center Use of Force Branch. For example, supervisor review ensures that the information entered does not contain administrative errors, that the narrative is clear, and, if able to compare against arrest reports related to the incident, the information is accurate. The legal and training reviews ensure that the actions reported fall within Secret Service eForce policy.

eForce also uses USSS personnel data from the ePerson system, rather than relying on personnel to manually input information about themselves or other involved personnel.

2.5 Privacy Impact Analysis: Related to Characterization of the

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES SECRET SERVICE, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE PERSON (EPERSON) SYSTEM, DHS/USSS/PIA-016 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-secret-service.

Information

Privacy Risk: There is a risk that inaccurate information may be entered into eForce because it is manually entered after an incident occurs.

Mitigation: This risk is mitigated. This information is reviewed by first- and second- line supervisors, certain members of the Office of the Chief Counsel Legal Training Section, and certain members of the James J. Rowley Training Center Use of Force Branch. This review process provides multiple steps to identify and correct inaccurate information. Incident information is collected at the scene of the incident, when appropriate and safe to do so. There may be times when information may need to be collected at another location such as a hospital or detention facility depending on the incident and situation. Personally identifiable information can be obtained from the subject; however, this information will be checked against any identification the subject has (e.g., driver's license, state ID card). Incident reports are required to be entered into eForce by the end of an agent/officer's shift of duty unless the incident resulted in death or serious bodily injury to an officer/agent or subject,[8] or a supervisor grants an extension (up to 10 days) in accordance with Secret Service eForce policy. Personally identifiable information entered into eForce should be compared against any incident reports to ensure the personally identifiable information is accurate.

Privacy Risk: There is a risk that more information than necessary may be entered into eForce, specifically the narrative space for incidents.

Mitigation: This risk is partially mitigated. The narrative space is used for describing incident details. Secret Service law enforcement personnel responsible for inputting details of the incident shall use this space solely for that purpose. Further, the narrative box specifies that users inputting information shall refrain from including unnecessary personally identifiable information within that space.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

As defined in Secret Service policy, information will be maintained in eForce to document agents/officers who are involved in reportable incidents and the subjects against whom force is used. The information entered into eForce will include full name, date of birth (of the subject), age, race, and gender to ensure that the agency complies with the reporting requirements in Executive Order 14074. The agency also analyzes the data on a quarterly basis to identify trends and determine if policies or training should be improved.

[8] In cases of death or serious bodily injury to an officer/agent and/or subject, eForce reporting may be delayed until after criminal and administration investigations are complete.

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.

On a quarterly basis, the Secret Service conducts internal data analysis to identify trends and evaluate whether policies or training should be changed. However, this is completed manually and the system is not used to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly about subjects or individuals.

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

No, access to eForce is limited solely to Secret Service employees and that access is further limited by their area of responsibility and assigned access levels within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk related to the potential misuse of personally identifiable information in eForce by Secret Service employees.

Mitigation: This risk is partially mitigated. Access to personally identifiable information that is maintained in eForce is limited to the entering agent/officer, their supervisors, and other reviewers (as discussed above). All personnel have received initial and recurrent training on the proper use and handling of personally identifiable information in conformance with Secret Service and DHS policies. Any Secret Service employee who is suspected of violating agency policy regarding the proper use and handling of personally identifiable information will be investigated in conformance with Secret Service policy and will receive appropriate discipline if misconduct is established.

Section 4.0 Notice

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

USSS agents/officers receive notice that their information may be collected and maintained if they are involved in a use of force incident. Subjects involved in a reportable use of force incident do not receive direct notice that their personally identifiable information will be entered into and maintained in eForce. However, the information entered into eForce about an individual involved in a use of force incident is the same information that will be collected for the incident report, which will also document the incident that resulted in the agent's/officer's use of force.

Information collected by the agent/officer involved in the reportable incident is done so with the awareness of the subject, usually at the time of the incident unless they are unaware of the situation due to injury or some other significant factor.

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

Agents/officers will not have an opportunity to opt-out or decline to provide their personally identifiable information as eForce reporting is required of all Secret Service agents/officers involved in a reportable incident. Notice is given to agents/officers regarding the inclusion of their personally identifiable information in eForce during training.

Subjects will not have an opportunity to opt-out or decline to have their personally identifiable information maintained in eForce. Additionally, the information maintained in eForce is the same information collected for the incident report. Subjects may refuse to give their name or date of birth to agents/officers; however, this information may be obtained at the holding facility as part of the arrest process if the subject is arrested.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that Secret Service employees and members of the public involved in a use of force incident may not be aware that their data is in eForce.

Mitigation: This risk is partially mitigated. All Secret Service employees are notified that if they are involved in a reportable incident, their information may be entered into eForce. This is reinforced through standard operating procedures and training. While agents/officers document the personally identifiable information of individuals involved in use of force incidents to include in the incident report, the individuals are not provided direct notice that their information will be maintained specifically in eForce. However, this Privacy Impact Assessment provides general notice of the use and purpose of the system.

Section 5.0 Data Retention by the Project

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

Per the NARA-approved schedule N1-087-11-005, eForce data will be cut off at the end of each calendar year, retained for 20 years, then transferred to NARA in five-year blocks (for example: data for 2023, 2024, 2025, 2026, and 2027 will be transferred to NARA in 2047).

eForce data not transmitted to the FBI or DHS on a recurring basis – including personally identifiable information – is treated as reference material as defined in N1-087-11-005, and will be destroyed "when no longer needed for administrative, legal, or audit purposes." This will be accomplished at the end of each calendar year, as part of the cut off process.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that personally identifiable information may be retained in eForce for a longer period than is necessary, based on the purpose for which the information originally was collected.

Mitigation: This risk is mitigated. A manual review will be required to identify any data elements that are eligible for disposal per the records retention guidelines. The Secret Service is working with its Office of the Chief Information Officer to add an automatic purge mechanism to eForce.

Section 6.0 Information Sharing

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.

Data related to use of force incidents that meet DHS and FBI reporting criteria will be provided to DHS and the FBI, respectively. Personally identifiable information will not be shared with outside agencies.

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

Personally identifiable information maintained in eForce is for internal use only. Personally identifiable information is not included in the use of force statistical data shared with DHS and the FBI.

6.3 Does the project place limitations on re-dissemination?

As noted, personally identifiable information is not shared with outside agencies.

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

The Enterprise Analytics Division will maintain a record of required disseminations of information.

6.5 Privacy Impact Analysis: Related to Information Sharing

There are no privacy risks associated with external information sharing because Secret Service does not share personally identifiable information maintained in eForce.

Section 7.0 Redress

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

Individuals seeking access to any record maintained in eForce or seeking to contest the accuracy of its content may submit a Privacy Act request to the Secret Service. Individuals, regardless of citizenship or legal status, may also request access to records under the Freedom of Information Act (FOIA). Access requests should be directed to the Secret Service Freedom of Information Act Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223 or FOIA@usss.dhs.gov. Requests will be processed under both the Freedom of Information Act and Privacy Act, as appropriate, to provide the requestor with all information that is releasable. Given the nature of the information in eForce, all or some of the requested information may be exempt from access to prevent harm to law enforcement investigations or interests.

Notwithstanding applicable exemptions, Secret Service reviews all information requests on a case-by-case basis. Instructions for filing a FOIA or Privacy Act request are available at http://www.dhs.gov/foia.

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

An individual who believes their information was improperly recorded in the system may submit a request through the Freedom of Information Act Office to have the information corrected.

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

Individuals are notified of the procedures for correcting their information through this Privacy Impact Assessment and as described at http://www.dhs.gov/foia.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access and/or correction requests for records in eForce.

Mitigation: This risk is partially mitigated. Individuals may make a Privacy Act or Freedom of Information Act request for Secret Service records including records in eForce. However, due to the nature of the records, they may be withheld for law enforcement or other purposes consistent with law.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in

accordance with stated practices in this PIA?

Secret Service policy defines reportable incidents and the associated reporting procedures. Further, law enforcement agents/officers are required to complete annual use of force refresher training which includes the requirement to enter reportable incidents in eForce.

Additionally, there are monthly audits of system logs to determine if there is any unusual activity occurring within the system. If unusual activity is detected, an investigation will take place to determine what has occurred. And if inappropriate activity is discovered, the responsible individual's access will be terminated and they may be subject to disciplinary action.

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

Secret Service employees are required to complete annual privacy awareness training regarding the use of personally identifiable information. Completion of this training is tracked through the USSS Office of Training.

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

Secret Service staff that possess a need-to-know will only be granted access to eForce based on the requirements of their assignment. System access is determined by job category. Only Secret Service agents and officers will have the ability within eForce to create use of force incident reports. Only the initiator of the use of force report can make changes to the report, and all changes are tracked and maintained in the system. Secret Service law enforcement supervisors may read the information and either concur with the report and forward it procedurally or return for corrections. Specific employees assigned to the Office of the Chief Counsel and the James J. Rowley Training Center Use of Force Branch will have read-only access to ensure that reported incidents conform with policy and training. USSS Office of Strategic Planning and Policy employees are granted access for reporting and analytical purposes only as needed.

Personnel within the Secret Service Office of the Chief Information Officer are responsible for setting permissions for access to eForce. Further, Office of the Chief Information Officer personnel may discover through a review of audit logs whether someone who should not have been granted access to eForce entered the system, which will immediately be remedied.

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?

This system is for Secret Service internal use only and personally identifiable information maintained in the database will not be shared with external partners.

Contact Official

John Shaffer
Program Manager, Assistant Special Agent in Charge
United States Secret Service
U.S. Department of Homeland Security

Responsible Official

Christal Bramson
Privacy Officer
United States Secret Service
U.S. Department of Homeland Security

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717