Drug Enforcement Administration

Office of Security Programs

Privacy Impact Assessment
for
CASTLE

Issued by:
David J. Mudd
Senior Component Official for Privacy
Drug Enforcement Administration

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: May 28, 2020

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

CASTLE is an Office of Security Programs initiative to provide security to all Drug Enforcement Administration (DEA) offices that is made up of two components. One component is a physical access control system to DEA facilities through proximity card credentials. The proximity card credentials use a commercial off the shelf application called "***CCure 9000***" developed by Softwarehouse, which is owned by Tyco. A proximity card credential is a contactless smart card which can be read without inserting it into a reader device, as required by earlier magnetic strip cards such as credit cards and "contact smart cards." The other component is closed-caption television (CCTV) recording and playback of DEA facility security cameras. CASTLE collects the date, time, and the specific door that was accessed by personnel, as well as their name and proximity card number. CASTLE also records video from security cameras. CCTV cameras collect possible gender, race, and/or ethnicity of personnel seeking to access DEA facilities. Since the CASTLE system does collect and maintain some forms of personally identifiable information (PII), DEA is required to complete a Privacy Impact Assessment (PIA) for its use of CASTLE, pursuant to the E-Government Act of 2002 and the Office of Management and Budget's (OMB) implementing guidance (OMB M-03-22).

Provide a non-technical overall description of the system that addresses:

(a) the purpose;

a.1). CASTLE validates that personnel attempting to access DEA facilities are authorized to do so through proximity card credentials and CCTV security cameras.

a.2). The recorded video is available for retrieval and review if there is a security incident which leads to a law enforcement investigation.

(b) how the information technology operates to achieve that purpose;

b.1). When users present their proximity card credentials at the proximity card reader, CASTLE compares the personnel credential/badge to information contained in DEA servers and permits access to entrance points by activating the locking hardware if the proximity badge matches that individual's authorized access rights.

b.2). CCTV cameras capture security video images in and around DEA facilities and store them on DEA servers.

(c) the general types of information involved;

c.1). CASTLE collects date, time, and the specific door that was opened by personnel, as well as their name and proximity card number.

c.2). CASTLE also records and maintains video and/or photos from security cameras for 30 days. CCTV cameras collect possible gender, race, and ethnicity of personnel seeking to access DEA facilities.

(d) how information may be used or shared;

d.1). Operators and Administrators both log into CASTLE using software installed onto their workstations located at their assigned occupied facilities to determine entry by personnel for reasons that may include audit purposes, or safety and security measures. Operators and Administrators can retrieve information from CASTLE by several parameters including name, date, time, proximity card number, and door name. The program has both database query and report functionality. Information is encrypted from each proximity card reader to the server across the network. Operators are responsible for updating access profiles and adding new profiles.

d.2). Recorded video can be searched using the Milestone XProtect client software installed onto the Operator's workstation and can be searched by camera location, motion, date, and time. CCTV videos are recorded via cameras located at each DEA Site and the video collected is stored locally on a recording computer at each DEA site. CASTLE records first-in/first-out; in other words, it rewrites over the oldest logged video after thirty days. The recorded video is available for review and retrieval, for up to thirty days, if there is a security incident this information may be considered necessary for use as evidence of a criminal act against the United States government.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

CASTLE validates that personnel attempting to access DEA facilities are authorized to do so. The CASTLE system provides protection to DEA employees, contractors, visitors, as well as DEA information and property by verifying that individuals entering DEA facilities have proper credentials. CASTLE accomplishes this using proximity card credentials as well as CCTV security cameras. CASTLE collects PII information to include the date, time, and specific door accessed by personnel, as well as their name and proximity card number. CASTLE also records video from security cameras of federal employees and contractors, as well as members of the public who may access the building or are recorded attempting to access DEA facilities. CCTV cameras collect possible gender, race, and ethnicity of people attempting to access DEA facilities. The collection of individual's names, work related information, and physical images is necessary to verify that individuals have appropriate credentials for the DEA facility they are entering. Unless there is a security incident which triggers a law enforcement investigation, the information described above is only accessed by the administrators and operators of the system. If there is a law enforcement investigation, relevant information would be disseminated to the investigating law enforcement agency and placed in a case file.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	40 U.S.C. § 1315
X	Executive Order	HSPD-12
X	Federal Regulation	41 CFR § 102-81.10
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	DEA Planning and Inspection Manual 8513-41.C.4

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	CCure
Date of birth or age			
Place of birth			
Gender	X	A, B, C, D	CCTV
Race, ethnicity or citizenship	X	A, B, C, D	CCTV - ***Not citizenship.***
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, D	CCure, CCTV – Entry access and recorded sightings.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	CCure, CCTV – Entry access and recorded sightings.
- **Video containing biometric data**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	A, B, C, D	CCTV
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**			
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	CCure, CCTV
- **Queries run**	X	A	CCure
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A	CCure – Proximity Card Number.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	Share with DEA Office of Professional Responsibility and DEA upper management for possible employee misconduct or criminal investigative purposes
DOJ Components	X			Share with FBI for possible criminal investigative purposes
Federal entities	X			
State, local, tribal gov't entities	X			Share with local police for possible criminal investigative purposes
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or

for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

CASTLE does not release information to the public for open data purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Overall consent is provided for badge credentials when applicants fill out an SF-86 for employment, (e.g. federal employees, task force officers, and/or contractors). Specifically, the SF 86 contains a page entitled "Authorization for Release of Information" which states: "I authorize the information to be used to conduct officially sanctioned and approved personnel security-related studies and analyses, which will be maintained in accordance with the Privacy Act".

The posted CCTV signs and requirements necessary for entry into the facilities is provided within locations visible for all to see, if the requested information is not provided, no access is given.

CASTLE's notices to the public are covered under system of records JUSTICE/DOJ-011, *Access Control System,* 69 Fed. Reg. 70279 (Dec. 3, 2004), 72 Fed. Reg. 3410, (Jan 25, 2007) (rescinded by 82 Fed. Reg. 24147), 82 Fed. Reg. 24147 (May 25, 2017) (amendment), and GSA-GOVT-7, HSPD-12 USAccess, 80 Fed. Reg. 64416, (Oct. 23, 2015).

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals do not have an opportunity to voluntarily provide consent, and without consent, proximity card credentials badge access into the facility or facilities is not obtained. In order for individuals to enter into DEA facilities they do not have the opportunity to consent to the collection of security camera footage. If they don't comply then access is not granted.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

The CASTLE system is only available to authorized Office of Security Programs, (ISPS) users that are designated as the "administrators" of CASTLE. This allows them to manage the application and administrator access to badge information, update individual photos, and video footage of all offices. Additionally, Designated Security Officers ("DSOs") also have access to CASTLE information. DSOs are located at each office responsible for the security

of the personnel assigned to their Division, District, Resident, or Post of Duty Office. A FOIA request can be made through the DEA FOIA office, however all information maintained in CASTLE is provided by the individual(s) to obtain a proximity card credential for access. For the photos collected by the CCTV cameras, there are no updates that can be made or requested, objects are captured in real time when in vicinity of the camera(s).

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** *ATO received on Jan 17, 2020 and expires on Jan23, 2023. ATO Recertification is current.* **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
N/A	**This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:**
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The security controls and risk posture are continuously monitored and evaluated. To safeguard and prevent the misuse of privacy information, assigned NIST 800-53, Rev 4 controls are tested and evaluated as part of the assessment process. The system connection is monitored on a constant basis to verify the enforcement of security requirements.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Access to CASTLE is protected by authentication controls, role-based permissions as only administrators or operators have access, and auditing features. To prevent unauthorized use, audit logs are maintained and verified during regular intervals and all operator and manager accounts are recertified on an annual basis through DEA's Account Management System. CASTLE system access is monitored by inspection of event logs, system logs, web logs, database application logs, and firewall logs.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. As a standard operating procedure, all

	contracts have the necessary, proper and accurate Privacy Act clauses and language required listed in each contract awarded within DEA.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** DEA follows the Annual Privacy training curriculum established by OPCL and is located on DEALS, DEA's on-line training forum.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Using DOJ's CSAM tool, the information type, Personal Identity and Authentication, were identified during the security categorization of the system, this particular information type has a Confidentially, Integrity, and Availability Federal Information Processing Standards (FIPS) 199 rating of Moderate overall. The controls regarding security and privacy are tested to ensure access and protection safeguards are in place to reduce the risk of compromise. The CASTLE system security plan, including administrative and technological controls, is documented in accordance with DOJ policy.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

The disposition standards for the Federal records in the CASTLE system are implemented and followed in accordance with the NARA retention schedule GRS 5.6 Security Records, Item 020 applies to Key and Card Access Accountability Records and Item 090 applies to Records of Routine Security Operations.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

___ No. _X__ Yes

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

JUSTICE/DOJ-011, *Access Control System,* 69 Fed. Reg. 70279 (Dec. 3, 2004), 72 Fed. Reg. 3410, (Jan 25, 2007) (rescinded by 82 Fed. Reg. 24147), 82 Fed. Reg. 24147 (May 25, 2017) (amendment), www.govinfo.gov/content/pkg/FR-2004-12-03/pdf/04-26590.pdf, and

GSA-GOVT-7, HSPD-12 USAccess, 80 Fed. Reg. 64416, (Oct. 23, 2015), https://www.govinfo.gov/content/pkg/FR-2015-10-23/pdf/2015-26940.pdf

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

a. Potential Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish the DEA's official duties is always a potential threat to privacy. CASTLE collects and maintains data information only about an individual that is relevant and necessary to accomplish CASTLE's functions. CASTLE source data information containing PII is collected at a minimum and is encrypted from each proximity card reader to the server across the network and are maintained for seven years. The date, time, and the specific door that was accessed by personnel, as well as their name and proximity card number are required to verify the individual attempting access to a DEA facility and have the authority to do so. CCTV video footage allows security officials to investigate unauthorized access to DEA facilities, or other security incidents that may occur. The CCTV videos that capture personnel and public entities are recorded on a first in first out basis and are written over after being maintained and stored at the DEA facility for 30 days. Unless a security incident occurs, the video segment is located and then saved to the case file.

b. Potential Threats Related to Use of the Information

Potential threats to privacy as a result of the DEA's use of the information in CASTLE include the risks of unauthorized access to the information, threats to the integrity of the information

resulting from unauthorized access or improper disposal of information, and unauthorized disclosure of the information. To prevent potential threats, access to CASTLE is granted only to DEA-approved Firebird authorized individuals who have signed a confidentiality agreement. The DEA also requires employees and contractors to undergo annual security and privacy training, and annually review and acknowledge DEA's rules of behavior to maintain their system access. Additionally, DEA personnel receive records training when entering on duty. Permission to the system is role-based and users are only authorized to access information on a need to know basis to perform their job duties. CASTLE exists on a physically secure, environmentally protected, internal network safeguarded by firewalls, and is administered by DOJ-approved contractor personnel.

c. Potential Threats Related to Dissemination

CASTLE will share information within DEA, DOJ, other Federal entities, and State and Local governments when required for evidence of possible criminal investigations and/or employee misconduct inquiries. CASTLE's connection to the Internet is firewall protected and communications to and from the server are encrypted via Secure Sockets Layer (SSL). DEA's firewall and operating system security are tested monthly. Patches are applied appropriately as required to maintain system integrity and security.

Consent is provided for proximity credentials when applicants fill out an SF-86 for employment, specifically the page Authorization for release of Information which states "I authorize the information to be used to conduct officially sanctioned and approved personnel security-related studies and analyses, which will be maintained in accordance with the Privacy Act". The posted CCTV signs for entry into the facilities are provided within locations visible for all to see.