U.S. Securities and Exchange Commission

Kastle Secure for Government (KS4G)
PRIVACY IMPACT ASSESSMENT (PIA)

August 30, 2023

Office of Support Operations

Section 1: System Overview

1.1 Name of Project or System

Kastle Secure for Government (KS4G)

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally Hosted (Contractor or other agency/organization)

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed:	5/23/2011
Last updated:	4/1/2022
Description of update:	Migration to Amazon AWS Cloud

1.4 Does the system or program employ any of the following technologies?

☒ Enterprise Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☒ Cloud Computing Services

☒ Web Portal - myKastle

☐ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

Kastle Systems is a security service provider of access control, video security, fire and life security, intrusion detection, and environmental control. The purpose of the system is to enable customers to provide and manage security to buildings and facilities by logging in remotely through a portal. The SEC Office of Security Services (OSS)/ Office of Support Operations (OSO) uses Kastle Secure for Government (KS4G) across all SEC offices for integrated video (Video Monitoring System), access control (Physical Access Control (PAC) System), and alarm monitoring. KS4G provides OSS Physical Security and Emergency Management (PSEM) Operations Branch the ability to authenticate, validate, and monitor to ensure that only authorized individuals access SEC offices and facilities.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

The legal authorities that authorize the collection of source information are 5 U.S.C. 301; Federal Information Security Management Act of 2002, as amended (44 U.S.C. 3554), and Homeland Security Presidential Directive-12 (HSPD-12).

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No

2.4 Do you retrieve data in the system by using a personal identifier?

☒ Yes, there is an existing SORN

System of Records Notice (SORN) SEC-20 "Facilities Access Badge System"

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☒ No

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The primary privacy risk identified is that personal information collected may be accessed by individuals that do not have need-to-know for business purposes. This risk is mitigated by limiting access to KS4G to only authorized PSEM Operations Branch staff.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

☐ The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

☐ Social Security Number
☐ Taxpayer ID
☐ Employee ID
☐ File/Case ID

☐ Alien Registration
☐ Driver's License Number
☐ Passport Information
☐ Credit Card Number

☐ Financial Accounts
☐ Financial Transactions
☐ Vehicle Identifiers
☐ Employer ID

☒ Other: Federal Agency Smart Credential Number (FASC-N)

General Personal Data

☒ Name
☐ Maiden Name
☐ Alias
☐ Gender
☐ Age
☐ Race/Ethnicity
☐ Civil or Criminal History

☐ Date of Birth
☐ Place of Birth
☐ Home Address
☐ Telephone Number
☐ Email Address
☐ Education Records
☐ Zip Code

☐ Marriage Records
☐ Financial Information
☐ Medical Information
☐ Military Service
☐ Mother's Maiden Name
☐ Health Plan Numbers

☐ Other:

Work-Related Data

☐ Occupation
☐ Job Title
☐ Work Address
☒ PIV Card Information

☐ Telephone Number
☐ Email Address
☐ Certificate/License Number
☐ Fax Number

☐ Salary
☐ Work History
☐ Business Associates

☒ Other: Work location and Employee affiliation (e.g., Contractor, Employee, etc.)

NOTE: PIV card information is limited to the Federal Agency Smart Credential Number (FASC-N) and card expiration date, which authenticates the identity of the card holder and verifies the card is valid.

Distinguishing Features/Biometrics

☐ Fingerprints
☐ Voice Recording

☒ Photographs
☒ Video Recordings

☐ Genetic Information
☐ Voice Signature

☐ Other:

System Administration/Audit Data

☒ User ID
☐ IP Address

☒ Date/Time of Access
☒ Queries Ran

☐ ID Files Accessed
☐ Contents of Files

☒ Other: The email addresses of system administrators are tracked.

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

PII collected in 3.1 is necessary to authenticate, validate, revoke, and monitor access to ensure only authorized individuals have access to SEC facilities.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees
Purpose: Information is collected to provide employees routine or long-term access to SEC facilities.

☒ SEC Federal Contractors
Purpose: Information is collected to provide contractors routine or long-term access to SEC facilities.

☒ Interns
Purpose: Information is collected to provide interns routine or long-term access to SEC facilities.

☐ Members of the Public
Purpose:

☒ Employee Family Members
Purpose: Information is collected to provide routine or long-term access for employee family members (such as spouse), who have children enrolled in the onsite childcare center,

☐ Former Employees
Purpose:

☐ Job Applicants
Purpose:

☒ Vendors
Purpose: Information is collected to provide vendors, who have a business need to be onsite, routine, or long-term access to SEC facilities.

☐ Other:
Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

The information collected is limited to that required to create a profile including card information and a building access profile for SEC sites. Only PII necessary to track user access and manage access to SEC facilities is stored in KS4G. PII is not used for testing, training, and/or research efforts.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☒ Yes.
General Records Schedule (GRS)

- DAA-GRS-2021-0001-0001, 5.6: Security Records
- DAA-GRS-2017-0006-0003, 5.2: Transitory and Intermediary Records:

3.6 What are the procedures for identification and disposition at the end of the retention period?

GRS DAA-GRS-2021-0001-0001, 5.6: Security Records: Security administrative records are required to be retained for 3 years, but longer retention is authorized if required for business use.

GRS DAA-GRS-2017-0006-0003, 5.2: Transitory and Intermediary Records: Key and card access accountability records for all other facility security areas are required to be retained for 6 months after return of key, but longer retention is authorized if required for business use. Video stored on GENETEC and Avigilon servers is only maintained for 30 days.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☐ N/A

☐ Members of the Public

Purpose:

☒ Employees

Purpose: KS4G tracks employee access to SEC buildings and other areas within buildings.

☒ Contractors

Purpose: KS4G tracks contractor access to SEC buildings and other areas within buildings.

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The collection of PII in KS4G presents privacy risks of inadvertent disclosure and unauthorized access of nonpublic information. The risks are mitigated through access control which restricts system access to only authorized PSEM Operations Branch staff.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☐ Privacy Act Statement

☒ System of Records Notice

SORN SEC-20 (Facilities Access Badge System) is not provided to individuals prior to collection but is published in the Federal Register and available on the SEC's website, www.sec.gov.

☒ Privacy Impact Assessment

The KS4G PIA is not provided to individuals prior to collection but is available on the SEC website.

Date of Last Update:

☐ Web Privacy Policy

☒ Other notice:

There are notices outlining requirements of Title 41 of the Code of Federal Regulations posted at all entrances. These notices inform all individuals entering federal space of the right of the government to screen and control access at a federal facility. Notices alerting individuals to the use of video monitoring are posted at all entrances.

☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

There is no privacy risk related to notice provided because adequate notice is provided as identified in section 4.1.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

When SEC employees and contractors scan their PIV card on the PAC reader, KS4G verifies authorization for access based on credential information stored on the PIV card. Authorized OSS PSEM Operations Branch staff and Points of Contacts (POCs) in regional offices, typically Assistant Regional Director for Operations (ARDO) and Administrative Officer's (AO) staff, access video to monitor entry/exit activities of SEC facilities. In addition, video footage of security incidents and issues that were observed or reported are reviewed.

5.2 Will internal organizations have access to the data?

☒ Yes

Organizations: OSS/PSEM provides OHR, OIT, and Enforcement Lab monthly reader reports or specialized periodic reports. In addition, OIG is provided read-only access to information in KS4G for investigative purposes, as needed.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

The privacy risk from internal sharing is inadvertent or unauthorized disclosure of PII. The SEC mitigates this risk by limiting information provided to that which is within the scope of the report (i.e., a specific reader report only contains the access history for that specific reader). In addition, the risk is mitigated by access controls that restrict access to only authorized users.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes
Organizations: When necessary, law enforcement agencies are provided video footage specific to criminal-related incidents recorded by SEC cameras.

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

The risk to privacy from external sharing is mitigated because the PII and video footage are only shared pursuant to a routine use disclosure in SEC SORN-20, Facilities Access Badge System, with law enforcement agencies when requested for investigative or enforcement purposes.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☒ Directly from the individual. Name and photograph collected at time of card issuance; via cameras installed at SEC facilities
☒ Other source(s): Photographs are manually downloaded, when necessary, from the USAccess database and then are uploaded into Kastle.

6.2 What methods will be used to collect the data?

When an individual applies for employment or a contractor position at the SEC, information is collected from the individual and submitted to OSS Personnel Security (PERSEC) for suitability determination. If favorable suitability is determined, the onboarding process is initiated. For PIV card issuance, the employee or contractor's PIV is inserted into the Kastle enrollment station card reader. Photograph, name, and PIV card number populate into myKastle. For facility access cards (temporary cards issued to non-SEC employee daycare parents and certain contractors), this information is manually entered by OSS PSEM Staff. Video footage is collected directly from the source camera and does not contain audio.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

During enrollment, all information is verified by the individual and the registrar (OSS/PSEM personnel). Access profiles are periodically checked by OSS/PSEM personnel for accuracy. OSS/PSEM personnel who access video management system footage have the option to review and record sections of the footage but cannot alter the video footage.

6.4 Does the project or system process, or access, PII in any other SEC system?

☒ No

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

The privacy risk identified is the use of inaccurate or outdated information. This risk is minimized because information is provided by the individuals themselves, verified during the background investigation, and then uploaded into KS4G.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

SEC employees, contractors, and interns do not have the option to decline, consent to uses, or opt out of information collection related to KS4G. Information is populated in the system prior to the start of employment (or contract support) to ensure authorized individuals have access to SEC buildings.

7.2 What procedures are in place to allow individuals to access their information?

Individuals seeking access to their information in KS4G may contact OSS PSEM at (202) 551-2222 or contact the Freedom of Information Act (FOIA)/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or may submit a request online.

7.3 Can individuals amend information about themselves in the system? If so, how?

SEC employees, contractors, and interns cannot directly amend information about themselves in KS4G. However, they may contact OSS PSEM at (202) 551-2222 or contact the Freedom of Information Act (FOIA)/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or may submit a request online.

7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

The risks are lack of access to information and the inability to seek redress and correction. The risks are mitigated because an individual may request correction of information as discussed in section 7.2 and 7.3.

Section 8: Security

8.1 Can the system be accessed outside of a connected SEC network?

☒ Yes

If yes, is secured authentication required?	☐ No	☒ Yes	☐ Not Applicable
Is the session encrypted?	☐ No	☒ Yes	☐ Not Applicable

8.2 Does the project or system involve an online collection of personal data?

☒ No

8.3 Does the project or system use web measurement and/or customization technologies?

☒ No

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC staff and contractors receive initial and subsequent annual privacy awareness training, which outlines roles and responsibilities for proper handling and protection of PII. SEC Rules of the Road ensure that employees and contractors are aware of their security responsibilities and how to fulfill them.

9.2 Does the system generate reports that contain information on individuals?

☒ Yes

Card reader reports contain names and office/division (if applicable) of individuals who access an SEC facility.

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☒ Yes

9.4 Does the system employ audit logging or event logging?

☒ Yes

9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Residual risk related to PII in the system is the inadvertent handling or misuse of data. To minimize this risk, user accounts for employees are synched with Active Directory, and system privileges are granted based on defined roles.