Privacy Impact Assessment
for
Physical Security Management System

3/17/2020

System/Business Owner

L.A. Harding

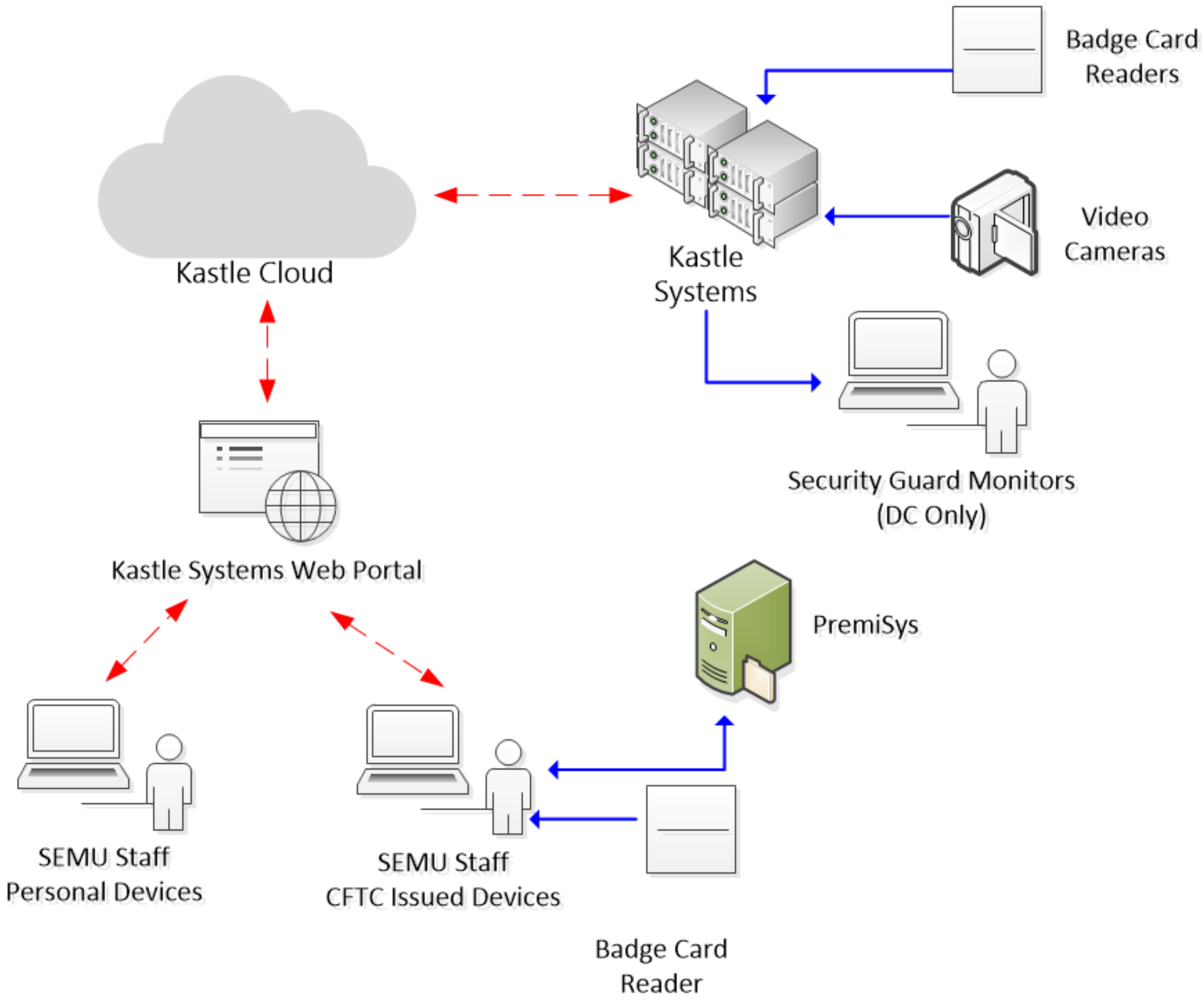
Reviewing Official
Charles Cutshall
Chief Privacy Officer
Commodity Futures Trading Commission

I. SYSTEM OVERVIEW

1) Describe the purpose of the system/collection:

   The Commodity Futures Trading Commission (CFTC) is responsible for the safety and security of its staff and property, including safeguarding its assets from potential loss or theft. To protect the safety and security of its staff and property, the CFTC has contracted with a 3rd party security management vendor (Kastle Systems) for the installation and management of badge card readers and security cameras in all of its office locations. The badging and camera systems provide an enhanced layer of security to manage individuals' access to CFTC offices and meet its responsibility to secure CFTC personnel, facilities, and information systems.

2) Provide a data map or model illustrating how information is structured or is processed by the system throughout its life cycle. Include a brief description of the data flows.


Badge Card Readers
Kastle Cloud
Kastle Systems
Video Cameras
Security Guard Monitors (DC Only)
Kastle Systems Web Portal
PremiSys
SEMU Staff Personal Devices
SEMU Staff CFTC Issued Devices
Badge Card Reader

Initial badge data is input into the CFTC badging system (PremiSys) by Security and Emergency Management Unit (SEMU) staff. This badge data is then uploaded to Kastle Systems by SEMU staff. This badge data comprises the initial access profile for an individual and is used to validate access against the badge holder when the badge is swiped. The Kastle System collects badge data when an individual swipes their card on a badge reader. For the DC office, when a badge is swiped at the front entrance, the individual's name, picture, and office location appear on the computer screen for the security guards to validate the individual's identity. For all other locations with badge readers, the system records the day and time the badge was swiped and this is linked to the individual's access profile in the Kastle System. Cameras are recording footage on the cameras' local memory at all times. Once the cameras detect motion, the footage is sent to the Kastle cloud for later review and investigation, if necessary. SEMU staff can view camera footage as well as staff access profiles via any web browser or the Kastle mobile application.

II. AUTHORITY AND PURPOSE

1) What is the legal authority to collect, use, maintain, and share information in the system?

- GSA Federal Management Regulations, Chapter 102, Sub-Chapter B
- Federal Property and Administrative Services Act of 1949 (as amended), §202, 40 USC 483(b)
- Office of Management and Budget (OMB)/Joint Financial Management Improvement Program Property Management System Requirements
- The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (November 2016/2nd Edition)
- The Federal Information Security Modernization Act of 2014 (FISMA 2014)
- Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors."
- Federal Information Processing Standard 201-2 (FIPS 201-2): Personal Identity Verification (PIV) of Federal Employees and Contractors

III. INFORMATION TYPES

1) What information will be collected, maintained, used, and/or disseminated?

Identifying Numbers	
☐ Social Security Number	☐ Truncated or Partial Social Security Number
☐ Driver's License Number	☐ License Plate Number
☐ Patient ID Number	☐ File/Case ID Number
☐ Student ID Number	☐ Health Plan Beneficiary Number
☐ Passport Number	☐ Federal Student Aid Number
☐ Employee Identification Number	☐ Taxpayer Identification Number
☐ Professional License Number	☐ Legal Entity Identifier

☐ Credit/Debit Card Number	☐ National Futures Association ID
☐ Personal Bank Account Number	☒ Other ID: HID ID#
☐ Personal Device Identifiers or Serial Numbers	
Contact Information	
☐ Personal Mobile Number	☐ Business Phone Number
☐ Personal E-mail Address	☐ Business E-mail Address
☐ Home Phone Number	☐ Personal or Business Fax Number
☐ Home Mailing Address	☐ Business Mailing Address
Sole Proprietors	
☐ Business Taxpayer Identification Number	☐ Business Mailing Address
☐ Business Credit Card Number	☐ Business Phone or Fax Number
☐ Business Bank Account Number	☐ Business Mobile Numbers
☐ Business Device identifiers or Serial Numbers	
Biographical Information	
☒ Name	☐ Gender
☐ Date of Birth	☐ City or County of Birth
☐ Country of Birth	☐ Zip Code
☐ Citizenship	☐ Military Service Information
☐ Spouse Information	☐ Academic Transcript
☐ Group/Org. Membership	☐ Resume or Curriculum Vitae
☒ Location Data – building and city	☐ Nationality
☐ Employment Information	☐ Marital Status
☐ Mother's Maiden Name	☐ Children Information
☐ Other: Time entry stamp	
Biometrics/Distinguishing Features/Characteristics	
☐ Fingerprints	☐ Height
☐ Retina/Iris Scans	☐ Voice/Audio Recording
☐ Hair Color	☐ Eye Color
☒ Video Recording	☒ Photos
☐ Weight	☐ Signatures
Active Directory/Device Information	
☒ IP Address	☒ MAC Address
☐ CFTC Asset Number	☐ Device Identifiers or Serial Numbers
☒ User Name	

IV. COLLECTING INFORMATION

1) How is the information in this system collected?

To create the initial access profile, information is collected directly from the individual's government-issued ID by SEMU staff and entered into Kastle Systems. Once an individual has an access profile, the system records the day, time, and location of where the badge is used. In the Washington, D.C. office, when an individual swipes their badge at the front desk, their photo, name, time stamp, and location where the badge was swiped appear on the screen for the security guard to validate the individual's identity.

The cameras record live video non-stop on a local memory card. Each camera is equipped with a motion sensor and once there is motion detected in the camera's view, the portion of the video that contains any motion activity is stored in Kastle Systems' secure cloud environment for later viewing and investigation.

V. INFORMATION USE

1) Will information in the system be retrieved using one or more of the data elements listed in Section III?

   In the course of an investigation badge data may be retrieved by an individual's name. For the camera footage, the information is stored by date and camera location, and cannot be retrieved by personal identifier.

2) If the information in the system is retrieved using one or more of the identifiers, what CFTC System of Records Notice (SORN) covers the information?

   The badge data is covered by CFTC-43, *Visitor Information System* (76 FR 5973)

VI. ACCESS AND SHARING

1) With which internal CFTC Offices or Divisions is the information shared? For each Office or Division, what information is shared and for what purpose?

   Access to the information in the system is limited to staff in the Security and Emergency Management Unit, and selected regional Logistics and Operations staff who require access to the information to perform their duties. In the event of an incident involving the theft or loss of property, a security incident related to the safety of CFTC staff or visitors, or any other incident that may necessitate identifying individuals, information in the system may be shared with Office and Division staff during the course of a response.

2) How is the information shared internally?

   The information is shared on a case by case and need to know basis. Information pertaining to a response will be shared internally via email and may be input into internal case management systems if tracked as part of an OIG or Legal case file.

3) With which external organization(s) is the information shared?

Kastle Systems has access to the information for technical support purposes as part of a services contract. In the course of responding to an incident the information may also be shared with Federal or local law enforcement.

4) How is the information shared externally?

The information is shared on a case by case and need to know basis. If in the course of responding to an incident information needs to be shared externally, it will be shared via email by encrypting the information in an attachment or otherwise transferring the information to secured external media with appropriate encryption.

VII. TRANSPARENCY

1) How are individuals notified as to how their information will be collected, used, and/or shared within this system?

Signs are placed in the areas where the cameras are recording video. In addition, this PIA and CFTC-33, Electronic Access Card 76 FR 5973 provide notice of the collection, use, and sharing of data from the system.

2) Is a SORN required? If so, explain how the use of the information in this system is limited to the use specified in the SORN?

A SORN is required for the badge information because an individual's name may be used to retrieve information. A SORN is not required for the camera footage because the information is not retrieved by a personal identifier and thus not stored as part of a Privacy Act system of records.

VIII. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

The name and HID ID are collected from CFTC's badging system. When an individual swipes their badge, the timestamp is collected directly from the individual. The camera footage is live footage recorded of the individual.

2) Is the collection mandatory or voluntary? If voluntary, what opportunities do the individuals have to decline to provide information?

The collection of the information is mandatory for an individual to receive a badge and gain access to the CFTC office. There are notice signs posted for the cameras, but an individual has no opportunity to decline being recorded once they enter an area monitored by a camera.

3) Do individuals have an opportunity to consent to a particular use of the information? If so, how do they provide consent for a particular use?

Individuals do not have an opportunity to consent to a particular use of their information.

IX. DATA MINIMIZATION

1) What steps were taken to minimize the collection of PII in the system?

The cameras are strategically placed in areas that require monitoring. In the Washington, D.C. office, the information the security guard views when an individual swipes their badge at the front desk is limited to only the information necessary to verify the individual’s identity (name, photo).

X. DATA QUALITY AND INTEGRITY

1) How is data quality ensured throughout the information lifecycle and business processes associated with the use of the information?

☐ Cross referencing data entries with other systems
☐ Third party data verification
☒ Data taken directly from individuals
☐ Character limits on text submissions
☐ Numerical restrictions in text boxes
☐ Other:

XI. RETENTION

1) What are the retention periods for the information?

Badge data (user profile including photo, access privileges, office location, and where the badge was swiped) is retained as long as the profile is active. Once the staff member using the badge is no longer employed or supporting the CFTC, the profile will be marked inactive by SEMU staff, and deleted 30 days later.

Video footage that is recorded on the local memory card of the camera that does not contain any motion activated activity is overwritten each time the card is full. Local memory cards can store approximately 30-35 days of footage. The footage that is activated by the motion sensor is stored for 90 days in the vendor’s cloud environment.

The records fall under General Retention Schedule (GRS) 5.6, item 090 for records of routine security operations. Video footage stored in the cloud is deleted after 90 days; however, specific footage involving an investigation or incident may be retained by SEMU for 3 years after final investigation or reporting action or when 3 years old, whichever is later, in accordance with GRS 5.6, item 100 for accident and incident records..

XII. SECURITY

1) What types of administrative safeguards protect the information?
☒ Contingency Plan
☐ User manuals for the system
☒ Rules of Behavior
☒ Non-Disclosure or other contractual agreement
☐ Other:

2) What types of physical safeguards protect the information?
☒ Guards
☒ Identification Badges
☒ Biometric
☒ Cameras
☒ Physically secured space with need to know access
☐ Other:

3) What types of technical safeguards protect the information?
☒ User Identification
☒ Firewall
☐ Virtual Private Network (VPN)
☐ Multi-factor Authentication (MFA)
☒ Passwords
☐ Encryption
☐ De-Identification
☐ Anonymization
☐ Other:

4) What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate use of the information?

Kastle Systems collects user access logs that indicate which users have accessed the system and the date and time of access. Only CFTC's SEMU and selected regional Logistics and Operations staff who function as SEMU representatives for their region can access the system.

5) Is this system hosted by a Cloud Service Provider (CSP)?
   a. If yes, which one?: Amazon Commercial Cloud
   b. If yes, has the system obtained a FedRAMP Authorization?: No

XIII. TRAINING

1) What privacy training is provided to users of the system?

   All CFTC staff receive mandatory annual privacy and cybersecurity training. There is no additional privacy-related training associated with the operation and use of this system.