Template Version Number: 01-2021

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Impact Assessment
for the
NOAA8868
Storm Prediction Center (SPC)

Reviewed by: Mark Graff Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

GRAFF.MARK.HYRUM.1514447892
Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2023.12.06 12:23:52 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

Template Version Number: 01-2021

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NWS/Storm Prediction Center (SPC)

Unique Project Identifier: NOAA8868

Introduction: System Description

The system is located in The National Weather Center, which completed construction in fall 2006. This $67 million state-of-the-science facility provides a collaborative environment in which University faculty, staff, and students work side-by-side with NOAA researchers and operational meteorologists. The NWC is part of the University's new Research Campus, which brings together academic, industry, and government organizations in a synergistic community. The new campus is designed to support round-the-clock mission-critical business needs and includes commercial buildings housing primarily weather and related companies.

The system is co-located with multiple NOAA Systems in the Computer Room located in a leased facility from the University of Oklahoma (OU) in Norman, OK. The primary NOAA tenant is the National Severe Storms Laboratory (NSSL) which is a FISMA low-impact system as the NOAA representative in all building-related issues with OU including but not limited to environmental control, physical security control, and other facility maintenance matters.

Forecast and Monitoring Support Systems: The Storm Prediction Center (SPC), located in Norman, OK, provides short and medium-range (0-8 days) weather forecasts, including severe convective, hazardous, and fire-related guidance and products for the contiguous United States. Products include, but are not limited to, outlooks, discussions, watches, and other guidance for heavy rain, heavy snow, severe thunderstorms, tornadoes, and fire-related weather events. SPC fire weather outlook products are for conditions favorable for wildfires in the contiguous US, for Day 1, 2, and 3-8, containing areas of critical or extremely critical fire conditions. These products are distributed directly to weather forecasting offices and, via distribution channels, to the emergency management community (emergency managers, police and fire departments, hospitals, utility companies, and response/relief organizations), other government and non-government agencies/groups, and the general public. SPC operational products are also made available to both public and private sectors through the SPC website. SPC utilizes NOAA WOC for public-facing web services and NOAA IDP for GIS services. There is no public access to the SPC system. The Forecasting and Monitoring Support Systems do not collect, store, or use any Personally Identifiable Information (PII) or Business Identifiable Information (BII).

The SPC operates multiple servers, workstations, local area networks, and other infrastructure components to provide forecasters with interactive, real-time access to a wide range of meteorological data. This data includes gridded numerical forecast products, observational data from Rawinsonde, METAR, aircraft, NEXRAD, satellite, and 'mesonet' networks, and the NWS AWIPS systems. There is no public access to these systems.

Administrative Systems: The SPC administrative systems support a variety of business activities required to establish and maintain budgeting, acquisition, facilities, and human resources management activities. Products consist of a variety of business memos, letters, forms, reports, and other similar documents and are produced on individual computers connected via networking to share common resources such as printers, storage farms, and e-mail. Only SPC personnel with access to any type of sensitive data provided by Office of Personnel Management, DOC, and NOAA systems have computers with non-networked local printers. There is no public access to any of SPC administrative systems.

Transmission of all the information from the video cameras monitoring of SPC restricted access areas occurs over an isolated layer 3 connection network segment using TLS 1.2 encryption to a NetApp storage device supporting the ViewCommander server. The NetApp device stores the video data on an isolated, FIPS 140-2 compliant, 256-bit

Advanced Encryption Standard (AES) encrypted volume. The ViewCommander video monitoring system sends email notifications to the spc.sysadmin@noaa.gov email distribution list of privileged SPC IT Specialists whenever a camera detects ingress/egress activity of SPC restricted access areas. The notification emails include four-frame motion clips from the live video stream for security review by the SPC IT Specialists.

Most of the data processed by SPC is scientific and results in impact-based decision support storm forecasting products and information that are made available to the meteorological and oceanographic community, public safety officials, and the general public. The computers, data, and information are important and critical to the accomplishment of the NOAA mission, and therefore this system is classified as high, mission-critical.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

General Support System

(b) System location

Norman, Oklahoma

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

- NOAA0201 – Web Operations Center
- NOAA3090 – National Severe Storms Laboratory (NSSL)
- NOAA8107 – Advanced Weather Interactive Processing System (AWIPS)
- NOAA8860 – Weather and Climate Computing Infrastructure Services (WCCIS)
- USAF – United States Air Force - NOAA Agreement

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The Storm Prediction Center (NOAA8868) operates using network infrastructure, virtual server infrastructure, physical servers, workstations, and storage area networks, and printers/faxes to support staff in meeting the mission. The SPC operates multiple servers, workstations, local area networks, and other infrastructure components to provide forecasters with interactive, real-time access to a wide range of meteorological data. This data includes gridded numerical forecast products, observational data from Rawinsonde, METAR, aircraft, NEXRAD, satellite, and 'mesonet' networks, and the NWS AWIPS systems. There is no public access to these systems. SPC utilizes the NOAA WOC for its external public-facing web services and NOAA/NWS Integrated Dissemination Program (IDP) for Geographic Information Systems (GIS) services to provide short and medium-range (0-8 days) weather forecasts, including severe convective, hazardous, and fire-related guidance and products for the public.

(e) How information in the system is retrieved by the user

SPC users can access SPC system information using Government Furnished Equipment (GFE) in conjunction with a Transport Layer Security (TLS) 1.2 encrypted Virtual Private Network (VPN) connection and appropriate federal/contractor user accounts. Other general weather-related information is received by the other interconnecting systems and public information can be accessed through the Trusted Internet Connection Access Point (TICAP) connection to the Internet. A non-privileged SPC user has no access to the output of the SPC restricted access area monitoring cameras. SPC management allows only certain specific employees (e.g. windows system administration) privileged access to the ViewCommander system to retrieve camera data.

(f) How information is transmitted to and from the system

Transmission of meteorological data between the interconnected systems utilizes FIPS 140-2 compliant SSH and TLS 1.2, and where possible TLS 1.3, transport encryption over private NOAA managed networks. Transmission of information from the restricted access area monitoring cameras to the NetApp storage device utilizes FIPS 140-2 compliant TLS 1.2 transport encryption over a private network segment within the SPC system. The video information is stored on the NetApp using FIPS 140-2 compliant 256-bit Advanced Encryption Standard (AES) encryption. This PII is only accessible to specified federal employees and contractors with system administration and security responsibilities for the SPC system.

(g) Any information sharing

This system collects and processes meteorological data using its forecasting and monitoring support systems. This includes weather forecasts, including severe convective, hazardous, and fire-related guidance. This information is distributed directly to weather forecasting offices and, via distribution channels, to the emergency management community (emergency managers, police and fire departments, hospitals, utility companies, and response/relief organizations), other government and non-government agencies/groups, and the general public. This is also done for both public and private sectors through the SPC website. SPC utilizes NOAA WOC for public-facing web services and NOAA IDP for GIS services. There is no public access to the SPC systems.

Transmission of information from the restricted access area monitoring cameras to the NetApp storage device utilizes FIPS 140-2 compliant TLS 1.2 transport encryption over a private network segment within the SPC system. The video information is stored on the NetApp using FIPS 140-2 compliant 256-bit Advanced Encryption Standard (AES) encryption. This PII is only accessible to specified federal employees and contractors with system administration and security responsibilities for the SPC system. This PII is only accessible to specified federal employees and contractors within the SPC system with authorized access to the ViewCommander system and its output. There is no public access to the SPC systems.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

- 5 U.S.C. § 301, Departmental regulations
- 15 U.S.C. 1512, Powers and duties of the Department of Commerce.
- 28 U.S.C. 533-535
- Executive Order 13356

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

HIGH

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

X___ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non- Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify The previous years' PTA incorrectly indicated an interconnection between NOAA8868 and NOAA0900 for the purposes of collecting PII/BII. The NOAA8868 system never had an interconnection with NOAA0900 and does not collect PII/BII for sharing with NOAA0900. No sensitive PII is collected. The previous PIA was wrong in stating that sensitive PII was collected.					

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name		h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	

e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address		i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording	X	i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify): Computer room security cameras.					

Government Sources

Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Video recording is in reference to the video surveillance at computer room ingress/egress points. While video surveillance is conducted at all ingress/egress points, a set of four frames from the video feed is only collected and sent as alerts when someone goes through the ingress/egress points of sensitive areas (i.e. computer room, satellite farm etc.). Accuracy is due to the presence of a person in view of the camera and correlation with log entries in the card key access system of access to restricted access locations.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities

Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): Video recording is in reference to the video surveillance at computer room ingress/egress points. While video surveillance is conducted at all ingress/egress points, a set of four frames from the video feed from the video feed is only collected and sent as alerts when someone goes through the ingress/egress points of sensitive areas (i.e. computer room, satellite farm etc.).			
	There is no IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.
(Check all that apply.)

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Photo snapshots (i.e. video frame grabs) from surveillance video are only to monitor entry and exit into the authorized areas, within the data center, UPS room, the satellite farm, the Main Distribution Frame (MDF), and the Intermediate Distribution Frame (IDF), since these areas contain essential Storm Prediction Center equipment and infrastructure.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The information that is captured is a video frame grabs from a video camera for security to a specific area within the data center, UPS room, the satellite farm, the MDF, and the IDF. The video frame grab is taken from the video surveillance and are used for alerting and audit purposes only. The video camera footage is stored on a highly restricted internal server with highly restricted access. This refers to all federal employees and contractors with access to these areas and cameras. None of the information is accessible to the public.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging

of information in accordance with the retention schedule, etc.)

Potential threats to privacy information are primarily the inadvertent disclosure of the information due to unauthorized access to the system or unintentional disclosure. Mitigations include the use of system security safeguards, which limits access to the information as well as monitors the access to the information system. Access to information is granted on a "need to know" basis and the least privilege principle. Users acknowledge the rules of behavior to ensure they understand their responsibilities. All employees also undergo annual IT Security and Privacy training to reduce the risk of unauthorized access or disclosure.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	*X		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

* The PII/BII in the system is only shared if necessary as part of an investigation of a security incident pertaining to access and activity in a restricted access location.

	The PII/BII in the system is not shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: ● NOAA0201 – Web Operations Center ● NOAA3090 – National Severe Storms Laboratory (NSSL) ● NOAA8107 – Advanced Weather Interactive Processing System (AWIPS) ● NOAA8860 – Weather and Climate Computing Infrastructure Services (WCCIS) ● USAF – United States Air Force The Storm Prediction Center prevents the accidental leakage of any PII due to internal security measures (network segmentation) that are employed within the SPC network boundary.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: .	
X	Yes, notice is provided by other means.	Specify how: Notice is provided using signs at the computer room ingress/egress points stating that there is video surveillance. Notice is provided through web banners prior to accessing the information system that any information provided (including BII/PII) is subject to safeguarding and proceeding to use the system and or provide information within the system indicates consent.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: SPC is in a leased facility from OU and OU clearly posts signs about occupants being recorded on video. Anyone may decline by leaving and avoiding any areas that are being video recorded. Anyone may also decline by not using any of the information system endpoints or portals.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: SPC is in a leased facility from OU and OU clearly posts signs about occupants being recorded on video. Consent is given upon entering the surveilled areas. Users have the opportunity to consent where warning banners are posted on endpoints or portals prior to providing any PII/BII.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: OU leases the space SPC resides in, and at external entrances, it is clear for people entering the building there will be video cameras throughout the building. This imagery is archived as a record of events occurring in the surveilled area. Individuals do not have the opportunity to review/update this imagery. Individuals only have the option of not entering SPC specified locations to prevent their information being collected. There is no option to request that the images be taken down.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:** The information that is being captured is stored on a secure internal server. Access to the server is extremely limited to only SPC personnel authorized by the System Owner or authorized SO designee (i.e, Supervisory IT Specialist).

X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 5/23/2023 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The information collected is stored on an internal SPC server that is configured with FIPS-140-2 encryption techniques. The server has a strongly restricted access list that is continuously monitored by the SPC IT Administrators.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g,, name or Social Security number)?

____ Yes, the PII/BII is searchable by a personal identifier.

X No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-13, Investigative and Security Records https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-13.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: General Records Schedule 5.6: The files are stored on local servers under strict security measures and are overwritten due to a lack of disk space.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing	X	Deleting	X
Other (specify): Data storage device destruction.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Images of personnel within the datacenter but no PII/BII metadata is collected in conjunction to attribute to a person in a video.
X	Quantity of PII	Provide explanation: PII collected is limited to only federal employees or contractors with authorized access to restricted access locations.
X	Data Field Sensitivity	Provide explanation: video recording and photographs.

X	Context of Use	Provide explanation: Video surveillance is captured to ensure the safety and security of employees and contractors.
X	Obligation to Protect Confidentiality	Provide explanation: SPC through privacy laws are obligated to ensure protection and confidentiality of any PII/BII within the system.
X	Access to and Location of PII	Provide explanation: The images are collected via an internal website and stored on a secured encrypted internal server. Only SPC system administrators are capable of viewing the live camera feeds. Any movement within the area will initiate a sequence frame that captures this information and is automatically emailed to SPC system administrators. In addition to security guards, only authorized employees and contractors with CAC cards are able to physically access these areas. Only employees and contractors with the appropriate role have access to any of the PII information collected by the system and must use their CAC in conjunction with their Government furnished equipment.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

SPC collects only the minimum required information necessary for the purpose in which it is intended. In addition, SPC participates in a mandated annual Assessment and Authorization (A&A) exercise that evaluates, tests, and examines security controls to ensure they are implemented in a way to adequately mitigate risk to unauthorized information disclosure. However, insider threats could potentially expose privacy data.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.