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

Privacy Threshold Analysis for the NOAA8868
Storm Prediction Center, SPC

U.S. Department of Commerce Privacy Threshold Analysis

NOAA – Storm Prediction Center

Unique Project Identifier: NOAA8868

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system:

The National Weather Center was completed in spring 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 two commercial buildings housing primarily weather and related companies. A third is currently under construction.

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, etc.

The center is also responsible for forecasting fire weather (conditions favorable for wildfires) in the contiguous US, and issues Day 1, 2, and 3–8 fire weather outlooks. These outlooks detail areas with critical or extremely critical fire conditions.

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, tornado, and fire-related weather events. 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. 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 system. The Forecasting and Monitoring Support Systems do not collect, store, or use any PII or 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 includes gridded numerical forecast products, observational data (Rawinsonde, aircraft, NEXRAD, satellite, and several '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 human resources, budgeting, acquisition, facilities, and management activities. Products consist of a variety of business memos, letters, forms, reports, and other similar documents and are produced on individual workstations utilizing commercially available business software, e.g. Microsoft Office Suite. These systems are connected via networking to share common resources such as printers, storage farms, and e-mail. However, the only computers with access to any sensitive data have non-networked local printers. There is no public access to these systems. Although most of the data is not sensitive, any sensitive data such as social security numbers are only stored externally within the Google environment in NOAA0900 (i.e. NOAA8868 collects SSNs but does not store them in NOAA8868, they are maintained in the SPC storage in NOAA0900). The other sensitive information is from the video cameras that is transmitted only as an encrypted live feed to a NetApp via an isolated layer 3 connection between the View Commander server and the NetApp. The stored data on the NetApp is an isolated and encrypted volume. These cameras are programmed to send email notifications including four frames per motion detected from the live stream when anyone passes through any ingress/egress points viewed by any of the cameras. Only the Administrative systems collect PII or BII and various security measures have been put in place to minimize the risk of privacy data leaks that include encryption at rest and in transit, least privileged access, and the above mentioned security cameras.

Most of the data processed is scientific and results in products and information that are made available to the meteorological and oceanographic community and the 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.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Address the following elements:

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

NOAA8868 is a 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 Scientific Computing Facility NOAA8107 - Advanced Weather Interactive Processing System
NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS)
NOAA0900 - Consolidated Cloud Applications
United States Air Force - NOAA Agreement

d) The purpose that the system is designed to serve

The Storm Prediction Center is tasked with forecasting the risk of severe thunderstorms and tornadoes in the contiguous United States. The agency issues convective outlooks, mesoscale discussions, and watches as a part of this process. Convective outlooks are issued for Day 1, Day 2, Day 3, and Day 4–8, and detail the risk of severe thunderstorms and tornadoes during the given forecast period, although tornado, hail, and wind details are only available for Day 1. Days 2 and 3, as well as 4–8 used a probabilistic scale, determining the probability for a severe weather event in percent. Mesoscale discussions are issued to give information on a region that is becoming a severe weather threat and states whether a watch is likely and details thereof, as well as situations of isolated severe weather when watches are not necessary. Watches are issued when forecasters are confident that severe weather will occur, and usually precede the onset of severe weather by one hour. The system also ensures proper human resource management for the employees within its boundary.

The center is also responsible for forecasting fire weather (conditions favorable for wildfires) in the contiguous US, and issues Day 1, 2, and 3–8 fire weather outlooks. These outlooks detail areas with critical or extremely critical fire conditions.

e) The way the system operates to achieve the purpose

The Storm Prediction Center (NOAA8868) operates with 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 includes gridded numerical forecast products, observational data (Rawinsonde, aircraft, NEXRAD, satellite, and several 'mesonet' networks, and the NWS AWIPS systems. There is no public access to these systems. SPC utilizes NOAA WOC for its external public-facing web services and NOAA IDP for 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. Other information used for human resource management such as taxpayer information and financial transactions are encrypted for transfer and storage within the system.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

Information from the camera to the storage device is transmitted over a private segmented network within the SPC system. This PII is only accessible to specified federal employees and contractors within the SPC system. Social security numbers are only collected and maintained in the NOAA0900 system and only accessible to specified federal employees and contractors. All other BIA in Section 2.1 are not shared and only accessible to federal employees and contractors within NOAA with access to financial records.

The system also collects 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 system.

g) Identify individuals who have access to information on the system

SPC internal personnel only, products are distributed through the SPC website that is hosted at the WOC and through AWIPS. Only the specified system administrator and system owner have access to the information (federal employees and contractors only).

h) How information in the system is retrieved by the user

A standard SPC user has no access to the output of the SPC cameras. SPC management allows only certain specific employees (e.g. windows sys administration) access to the system to retrieve data. System information can be accessed through Government Furnished Equipment (GFE) in conjunction with a 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 internet.

i) How information is transmitted to and from the system

Information from the camera to the storage device is transmitted over a private segmented network through SSL within the SPC system and stored encrypted on the NetApp storage. Social security numbers within the system are transmitted through encrypted/SSL and stored encrypted within the SPC boundary in NOAA0900. Other information on meteorological data transmission between the interconnected systems happens over SSL/private networks.

Questionnaire:

1. Status of the Information System.

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

_X_ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Video surveillance is now collected and stored by NOAA8868					

___ 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.
Continue to answer questions and complete certification.

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

_____ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

___ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X____ Yes. *(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 facility ingress/egress points. While video surveillance is conducted at all ingress/egress points, photograph snapshots from the video feed is only collected and sent as alerts when someone goes through the ingress/egress points of sensitive areas (i.e.			

Datacenter, satellite farm etc.).

_____ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII.

_____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- __X__ DOC employees
- __X__ Contractors working on behalf of DOC
- _____ Other Federal Government personnel
- _____ Members of the public

_____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

__X__ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated

form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. For human resource management purposes only. The SSN are not disseminated or used for any other purposes.
Provide the legal authority which permits the collection of SSNs, including truncated form. 15 U.S.C 1501 et seq. – Department of Commerce 44 U.S.C. 3101 – Records management by agency heads; general duties

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

_____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to the NOAA8868 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the NOAA8868 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Cardozo W. Shu Office: NWS/NCEP/SPC Phone: 240-621-2472 Email: Cardozo.Shu@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: SHU.CARDOZO.WARRICK.1598125364 Digitally signed by SHU.CARDOZO.WARRICK.1598125364 Date: 2022.10.26 15:07:39 -04'00' Date signed: 10/26/2022	**Information Technology Security Officer** Name: Andrew Browne Office: NWS ACIO Phone: 301-427-9033 Email: Andrew.browne@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2022.10.26 15:19:08 -04'00' Date signed: 10/26/2022
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2022.11.23 07:44:51 -05'00' Date signed: 11/23/22022	**Authorizing Official** Name: Michael Farrar Office: NWS NCEP Phone: 301-683-1315 Email: Michael.farrar@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: FARRAR.MICHAEL.RAY.1106463960 Digitally signed by FARRAR.MICHAEL.RAY.1106463960 Date: 2022.11.20 15:17:10 -05'00' Date signed: 11/20/2022
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.11.30 10:31:46 -05'00' Date signed: 11/30/22	