Template Version Number: 01-2021

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

## Privacy Impact Assessment
## for the
## NOAA0301
## Traffic Coordination System for Space (TraCSS)

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

JENNIFER GOODE Digitally signed by JENNIFER GOODE
Date: 2025.06.20 14:12:33 -04'00'

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

# U.S. Department of Commerce Privacy Impact Assessment
# NOAA/Office of Space Commerce/Traffic Coordination System for Space

**Unique Project Identifier: NOAA0301**

**Introduction: System Description**

The Office of Space Commerce's (OSC) Traffic Coordination System for Space (TraCSS) serves as the Department of Commerce's (DOC) comprehensive, enterprise solution for the ingestion, processing, long-term archiving, and real-time dissemination of Space Situational Awareness (SSA) data and analytical products. Designed to ensure the safety, sustainability, and strategic advancement of U.S. space assets, TraCSS delivers critical conjunction assessment and collision avoidance services to commercial satellite owner/operators (O/Os). By leveraging advanced orbital mechanics algorithms, data fusion techniques, and predictive modeling, the system supports timely decision-making to mitigate the risk of on-orbit collisions.

TraCSS aggregates and correlates large volumes of orbital data sourced from multiple authoritative entities, including the Department of Defense (DoD), Department of State, the National Oceanic and Atmospheric Administration

(NOAA), U.S. commercial SSA data providers, civil and commercial satellite operators, and select international governmental and civil partners. The system is designed to be interoperable with both legacy and emerging space traffic management standards and protocols, ensuring compatibility across diverse orbital regimes and mission types.

Operating continuously on a 24x7x365 basis, TraCSS is engineered for high availability, redundancy, and secure access. It supports national space policy objectives by promoting transparency, fostering innovation in SSA technologies, and bolstering the global competitiveness of the U.S. commercial space industry through reliable space traffic coordination and data sharing capabilities.

Address the following elements:

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

TraCSS is a general support system.

*(b) System location*

TraCSS is part of the Amazon Web Services (AWS) government cloud located in the east and western parts of the United States, including office locations in Washington D.C.; Suitland, Maryland; and Boulder, Colorado.

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

TraCSS connects to other NOAA systems including:

- NOAA0100 – NOAA Cyber Security Center (NCSC)
- NOAA1200 – Corporate Services (CorpSrv) Local Area Network (LAN) (specifically Boulder, Colorado; and Suitland, Maryland LAN locations)
- NOAA0201 – NOAA Web Operations Center (WOC)
- NOAA0220 – NOAA Cloud Management System
- NOAA0550 – NOAA N-Wave Enterprise Network
- NOAA0700 – NOAA High Availability Enterprise Services (HAES)

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

TraCSS consists of TraCSS-OASIS, a data repository that ingests and stores information on resident space objects, and TraCSS-SKYLINE, an application layer that leverages TraCSS-OASIS data to perform analysis and provision SSA services, such as conjunction analysis. The TraCSS-HORIZON Modeling, Analysis, Simulation, Test, Evaluation, and Research (MASTER) and Development and Test (DevTest) environments facilitate the entire lifecycle of system development, from initial modeling and analysis to final testing and evaluation, and ongoing research.

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

Information in the TraCSS is retrieved through an Access Control List (ACL), which ensures that only authorized users with a legitimate need to know can access specific data. Access to the system is managed through an identity management service, which users must use to authenticate and gain access. The ACL ensures that data is restricted according to user roles and permissions, providing secured and controlled access to sensitive information.

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

The information is transmitted to and from the system using Advanced Encryption Standard (AES) 256 encryption.

*(g) Any information sharing*

The TraCSS collects information on resident space objects from a variety of sources, which includes importing unclassified data from the DOD such as trajectory information and other data on space objects (satellites and space debris), performing quality checks on the data, and estimating if there are any close approaches. The information includes metadata (satellite characteristics) on satellites and their operational characteristics and SSA products generated by third-party applications procured from commercial providers. If satellites come too close to one another, NOAA shares the satellites' POC information with the satellites' operators allowing them to notify each other about the proximity and request adjustments to prevent a collision.

*(h) The specific programmatic authorities (statutes or Executive Orders) for collecting,*

*maintaining, using, and disseminating the information*

| |
|---|
| 5 USC 301, Departmental Regulations |
| 15 U.S.C. 1512, Powers and duties of Department |

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

The FIPS 199 security impact category for the TraCSS is “High.”

## Section 1: Status of the Information System

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

_X_ This is a new information system.

_____ 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): | | | | | |

____ 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 | X | 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. Sex | | k. Telephone Number | X | r. Criminal Record | |
| e. Age | | l. Email Address | X | 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 | X | e. Work Email Address | X | i. Business Associates | |
| b. Job Title | X | f. Salary | | j. Proprietary or Business Information | X |
| c. Work Address | X | g. Work History | | k. Procurement/contracting records | |
| d. Work Telephone Number | X | 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 | | i. Height | | n. Retina/Iris Scans | |
| e. Photographs | | j. Weight | | o. Dental Profile | |
| p. Other distinguishing features/biometrics (specify): | | | | | |

| **System Administration/Audit Data (SAAD)** | | | | | |
|---|---|---|---|---|---|
| a. User ID | X | c. Date/Time of Access | X | e. ID Files Accessed | X* |
| b. IP Address | X | d. Queries Run | | f. Contents of Files | |
| g. Other system administration/audit data (specify): *Files Accessed is selected because all access to PII/BII files are tracked. The system logs every instance of file access, creating an audit trail for security monitoring and compliance auditing. These logs help detect unauthorized access, ensure that only authorized personnel are viewing or editing sensitive information, and support investigations in case of a breach. | | | | | |

| **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 | | Hard Copy: Mail/Fax | | Online | X |
| Telephone | X* | Email | X | | |
| Other (specify): * If a user does not want to provide their information via email, they can call NOAA and provide the relevant information. | | | | | |

| Government Sources | | | | | |
|---|---|---|---|---|---|
| Within the Bureau | X | Other DOC Bureaus | X | Other Federal Agencies | X |
| State, Local, Tribal | | Foreign | X* | | |
| Other (specify): *These individuals are satellite operators from other countries. | | | | | |

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

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

| |
|---|
| The system has a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to, data validation controls to ensure accuracy of information. The system information is entered by the system O/Os. The information is then verified by a TraCSS employee or contractor. |

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| X | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection.<br><br>NOAA has initiated the PRA process for this new collection of information. |
| | 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 | X |
| Other (specify): The system developers have access to the system using PIV cards. | | | |

| | |
|---|---|
| | 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 | | Electronic purchase transactions | |
| Other (specify): | | | |

| | |
|---|---|
| X | There are not any 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 | X |
| 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) | X | For web measurement and customization technologies (multi-session) | |
| Other (specify): | | | |

## 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 Personally Identifiable Information (PII) and Business Identifiable Information (BII) collected, maintained, or disseminated by TraCSS support various functional areas, including access control, audit logging, and operational oversight. This data is critical for ensuring secure system access, maintaining accountability, and supporting the broader mission of space situational awareness.

The PII/BII referenced includes data from the following groups:

- Federal Employees and Contractors: Used to verify identity, manage access privileges, and

log system activity for compliance with federal security policies.

- American Companies: Utilized for business operations, including data-sharing agreements, ensuring appropriate access control, and maintaining the integrity of shared data.
- Foreign Companies: Collected to facilitate international cooperation in space operations, ensuring data security and adherence to applicable regulatory frameworks.

This information is used primarily to:

1. Support Access Controls: Ensure that only authorized users can access specific system functions and data, using role-based permissions. Account users can review and update their PII/BII at any time by accessing their account settings on the website. Clear, step-by-step instructions are provided to guide users through updating personal details such as contact information, preferences, or other relevant data. Users also receive periodic reminders to verify and update their information to ensure accuracy.

2. Enable Audit Logging: Record and monitor user activities to detect unauthorized access, ensure compliance, and maintain system integrity. In cases where specific updates require verification, such as changes to sensitive data (e.g., legal name or email), users are required to provide authentication or supporting documentation.

3. Populate TraCSS: Facilitate data integration from various sources to enhance operational capabilities, such as tracking space objects and providing situational awareness insights. All updates are processed promptly, and changes are reflected in the system immediately or within a specified timeframe, which is communicated to the user. These practices ensure that individuals maintain control over the accuracy and completeness of their PII/BII.

By securely managing PII/BII in accordance with federal regulations and best practices, the TraCSS ensures that sensitive information is handled responsibly while supporting its critical mission objectives.

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.)

The use of data by the Office of Space Commerce (OSC) presents potential privacy threats, particularly insider threats, which include both malicious and unintentional actions by employees or contractors. These risks are mitigated through a comprehensive Defense in Depth strategy,

where multiple layers of security are deployed to protect data at every level, ensuring that no single point of failure can compromise the system.

Potential Threats

1. Malicious Insiders: Employees or contractors deliberately seeking to steal, misuse, or damage sensitive information.

2. Negligent Insiders: Individuals who unintentionally cause data breaches by mishandling information or falling victim to phishing attacks.

To address these threats, the OSC and NOAA implement an extensive set of technical, administrative, and procedural controls as part of a holistic approach to data protection.

Defense in Depth Strategy

1. Mandatory Training and Awareness Programs

NOAA enforces annual Cyber Security Awareness Training for all employees and contractors, which includes:

- Proper data handling, storage, and dissemination protocols.
- Insider threat awareness, including recognizing phishing, social engineering, and other risks.
- Procedures for secure data disposal in line with record retention schedules.

These initiatives ensure that all personnel understand their roles in safeguarding sensitive information.

2. Multiple Layers of Security Controls

The TraCSS employs a variety of NIST 800-53 compliant controls to protect PII/BII at every stage, ensuring that no single security breach can compromise the entire system:

Perimeter Security Controls:

- Intrusion Detection and Prevention Systems (IDS/IPS) monitor and block unauthorized access attempts.
- Firewalls act as barriers to filter and control network traffic.

Network Security Controls:

- Trusted Internet Connection (TIC) ensures all traffic is routed through secure gateways.
- Encryption (AES-256) protects data in transit, ensuring confidentiality during transmission.

Endpoint Security Controls:

- Anti-Virus and Endpoint Detection & Response (EDR) systems protect devices from malware and malicious activity.
- Homeland Security Presidential Directive 12 (HSPD-12) Compliant PIV Cards enforce strong multi-factor authentication for system access.

Data Security Controls:

- Database encryption ensures data at rest is secured with AES-256 encryption.
- Automated data purging follows record retention schedules to securely remove outdated data.

3. Cloud Security and Compliance

The TraCSS's cloud environment is certified under the Federal Risk and Authorization Management Program (FedRAMP) and adheres to FISMA standards, ensuring:

- Continuous security monitoring and assessments.
- Standardized risk management processes.
- Encryption and access controls that meet stringent federal security requirements.

4. Monitoring and Audit Logging

OSC employs continuous monitoring and comprehensive audit logging to detect, respond to, and mitigate threats in real time:

- Audit logs track all user activities, providing a detailed record of data access and system interactions.
- Security Information and Event Management (SIEM) tools aggregate and analyze log data for potential anomalies or security incidents.

5. Incident Response and Contingency Planning

In the event of a security incident, OSC has an established Incident Response Plan (IRP) that includes:

- Immediate containment and remediation of the breach.
- Notification procedures to inform relevant stakeholders.
- Post-incident analysis to strengthen future defenses.

The OSC's Defense in Depth approach ensures robust protection of PII and BII by implementing multiple, redundant security layers. From mandatory training and endpoint protection to continuous monitoring and secure data disposal, OSC effectively mitigates insider threats while maintaining the integrity, confidentiality, and availability of critical information.

## 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 | X | | |
| Federal agencies | | | X |
| State, local, tribal gov't agencies | | | |
| Public | | | |
| Private sector | X | | |
| Foreign governments | X* | | |
| Foreign entities | | | |
| Other (specify): | | | |

The PII/BII in the system is shared so that satellite owners can move their satellites if they are too close to each other.

* "Foreign Governments" is selected to indicate that PII/BII are being shared with foreign governments as required by law or through international agreements, with strict adherence to data protection measures. The information is securely transmitted, ensuring compliance with relevant privacy regulations and safeguarding the individuals' rights. The purpose of sharing this data is primarily for specific purposes, such as national security (e.g., the moving of satellites), public safety, and international cooperation.

| | |
|---|---|
| | The PII/BII in the system will not be shared. |

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

| | |
|---|---|
| X | 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. |
| | 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.

| | |
|---|---|
| | Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:<br><br>TraCSS connects to other NOAA systems including:<br>• NOAA0100 – NCSC<br>• NOAA1200 – CorpSrv LAN<br>• NOAA0201 – NOAA WOC<br>• NOAA0220 – NOAA Cloud Management System<br>• NOAA0550 – NOAA N-Wave Enterprise Network<br>• NOAA0700 – NOAA HAES<br><br>TraCSS Cloud Services receives authentication information from NOAA's Identity and Access Management capabilities. The IT system uses a multitude of security controls mandated by the FISMA and various other regulatory control frameworks including the NIST special publication 800 series. These security controls include, but are not limited to, the use of mandatory |

| | |
|---|---|
| | Hypertext Transfer Protocol Secure (HTTPS) for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at NOAA that house information systems. |
| | 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:<br><br>. | |
| X | Yes, notice is provided by other means. | Specify how:<br><br>BII is shared through formal user agreements established between the system's users and the OSC. These agreements outline the terms, conditions, and responsibilities for accessing and utilizing TraCSS, including provisions related to the collection, use, and protection of BII. Users are required to acknowledge and consent to these terms before accessing the system, ensuring transparency and understanding of how their data is handled.<br><br>In addition, account-related content is available on the official TraCSS website at https://www.space.commerce.gov/traffic-coordination-system-for-space-tracss/, where users can:<br>1. Access Privacy Information:<br>• Review detailed privacy policies outlining how BII is collected, stored and shared.<br>• Understand their rights regarding data access, correction, and retention.<br>2. Review User Agreements and Terms of Use:<br>• Obtain copies of the user agreements they've |

| | | |
|---|---|---|
| | | consented to, ensuring continuous awareness of data-sharing policies.<br>3. Manage Account Information:<br>• Update personal or business-related information securely.<br>• View data access logs or notifications related to data use.<br><br>By leveraging user agreements and the TraCSS.gov platform, the OSC ensures that all users are fully informed about the use and dissemination of their BII, promoting transparency, accountability, and compliance with applicable privacy regulations. |
| | 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:<br>Individuals are informed that providing PII is optional and they can choose not to disclose this information. |
| | 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:<br>Proprietary data is provided under clearly defined agreements, such as data-sharing agreements, user licenses, or terms of service. These agreements specify the purpose for data collection, the types of data collected, the methods of data processing, and any third parties with whom data may be shared. Consent is obtained explicitly at the time of agreement through signed contracts or by accepting terms electronically.<br>For account users, the consent process occurs during account registration. Users are presented with the organization's privacy policy and terms of use, which outline how their PII/BII is collected, used, stored, and shared. By completing the account setup, users acknowledge and consent to the stated data practices.<br>Additionally, users have options to manage or modify their consent preferences, such as opting out of certain data uses, where applicable. Regular updates to the privacy policy are communicated to users, ensuring continued informed consent |

| | | |
|---|---|---|
| | | for any changes in data usage. |
| | 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.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to review/update PII/BII pertaining to them. | Specify how:<br>Account users can review and update their PII/BII at any time by accessing their account settings on the website. Clear, step-by-step instructions are provided to guide users through updating personal details such as contact information, preferences, or other relevant data. Users also receive periodic reminders to verify and update their information to ensure accuracy.<br>In cases where specific updates require verification, such as changes to sensitive data (e.g., legal name or email), users are required to provide authentication or supporting documentation.<br>All updates are processed promptly, and changes are reflected in the system immediately or within a specified timeframe, which is communicated to the user. These practices ensure that individuals maintain control over the accuracy and completeness of their PII/BII. |
| | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not: |

## Section 8: Administrative and Technological Controls

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

| | |
|---|---|
| X | All users signed a confidentiality agreement or non-disclosure agreement. |
| X | 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.<br>**Explanation:** Access to PII/BII is monitored, tracked, and recorded to ensure data security and compliance with privacy regulations. The system records and audits all access to sensitive information, including identifying the individuals accessing the data, the times of access, and the actions performed on the records. This ensures that any unauthorized or inappropriate access can be quickly identified and addressed.<br><br>Rationale for Selecting "Files Accessed":<br>In Section 2.1, Files Accessed is selected because all access to PII/BII files are tracked. The system logs |

| | |
|---|---|
| | every instance of file access, creating an audit trail for security monitoring and compliance auditing. These logs help detect unauthorized access, ensure that only authorized personnel are viewing or editing sensitive information, and support investigations in case of a breach.<br>Why This Is Important:<br>• Data Protection: Helps safeguard PII/BII from unauthorized access or misuse.<br>• Compliance: Ensures adherence to legal and regulatory requirements for data security and privacy.<br>• Accountability: Establishes clear records of who accessed the data and when, enhancing transparency and accountability.<br>• Incident Detection: Allows for prompt identification of any unusual or suspicious access patterns that could indicate a security breach. |
| X | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): August 18, 2024<br>☐ 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. |
| X | Contracts with customers establish DOC ownership rights over data including PII/BII. |
| X | 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 OSC IT TraCSS employs a multitude of layers and security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- IDS | IPS
- Firewalls
- Use of TIC
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls: AWS provides several security capabilities and services to increase privacy and control network access which include the following: OSC uses encryption at rest settings for AWS storage resources. Encryption keys are stored within a FIPS 140-2 standard validated key store. Data in transit is encrypted using Transport Layer Security (TLS) connections to endpoints. Communications that traverse the account boundary of the TraCSS environment routes through the N-Wave Virtual Private Network (VPN) Gateway that provides IP Security (IPSEC) tunnel communications between the TraCSS

environment and external communications. Network Access Controls are configured to allow only trusted network subnets access to OSC network segments. Security group configurations isolate network resources based on IP addresses, ports, and protocols. TraCSS utilizes data analytics resources to provide end-to-end data security. The analytics uses a holistic approach security feature that includes:

- Administration
- Authentication and perimeter security
- Authorization
- Audit
- Data protection

## 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."

| | |
|---|---|
| | Yes, this system is covered by an existing system of records notice (SORN).<br>Provide the SORN name, number, and link. *(list all that apply)*: |
| | Yes, a SORN has been submitted to the Department for approval on (date). |
| X | No, this system is not a system of records and a SORN is not applicable.<br>The system does not utilize personal identifiers such as names, Social Security numbers, or other unique personal identifiers to search or retrieve data. Instead, data is indexed and accessed through alternative methods, such as system-generated identification numbers, anonymized data sets, or aggregated information. This approach ensures that PII/BII remains protected and aligns with privacy-by-design principles, minimizing the risk of unauthorized access or disclosure of personal information. |

## 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.)*

| | |
|---|---|
| | There is an approved record control schedule.<br>Provide the name of the record control schedule: |
| X | No, there is not an approved record control schedule.<br>Provide the stage in which the project is in developing and submitting a records control schedule:<br><br>The project is currently in the process of developing a records control schedule. This involves reviewing the types of records being generated, assessing their retention requirements based on applicable laws, regulations, and organizational policies, and ensuring alignment with the broader records management framework. Once the schedule is finalized, it is be submitted for approval to ensure compliance with legal and regulatory requirements. |
| | 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 | | Deleting | X |
| Other (specify): | | | |

## 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.)*

| | |
|---|---|
| | Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. |
| X | 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: PII/BII stored/maintained can be used to directly identify individuals. |

| | | |
|---|---|---|
| X | Quantity of PII | Provide explanation: The only PII is account contact information. |
| X | Data Field Sensitivity | Provide explanation: No sensitive PII is collected. The primary PII collected in this system is account contact information (e.g., names, email addresses, phone numbers, and mailing addresses).<br><br>BII includes unclassified data from the DOD, such as trajectory information and other data on space objects (satellites and space debris), and metadata (satellite characteristics) on satellites and their operational characteristics and SSA products generated by third-party applications procured from commercial providers.<br>A breach of this data could undermine trust in the organization's ability to protect personal information, damaging its reputation and relationships with stakeholders. |
| X | Context of Use | Provide explanation: Disclosure of the PII/BII in this IT system could result in severe harm to the individual or organization. |
| X | Obligation to Protect Confidentiality | Provide explanation: PII/BII collected is required to be protected in accordance with Privacy laws. |
| X | Access to and Location of PII | Provide explanation: The PII is physically located on the cloud. The TraCSS is operating on the AWS Govcloud. ACL ensures that data is restricted according to user roles and permissions, providing secured and controlled access to sensitive information. |
| | 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.)

The collection of PII is required for the TraCSS program. Therefore, some individuals would be affected if there was loss, theft, or compromise of the data. TraCSS is hosted on the AWS GovCloud environment. TraCSS is accessed by authorized individuals that have a business need to know.

NOAA conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible. In addition to the security protocols already described in this assessment, NOAA and OSC limit access to sensitive information to sworn employees who have an authorized business need to know. In order to offer the maximum-security protection to OSC users and stakeholders, the TraCSS cloud environment is FISMA certified. These NIST 800-53 controls, at a minimum, are deployed

and managed at the enterprise level including, but not limited to the following:

- IDS | IPS
- Firewalls
- Use of TIC
- Encryption of databases (Data at rest)
- Access Controls: NOAA information technology systems also follow the NIST standards including special publications 800-53, 800-63, 800-37 etc. Any system within NOAA that contains, transmits, or processes PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended.

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.<br>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.<br>Explanation: |
| X | No, the conduct of this PIA does not result in any required technology changes. |