



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

Affects Members Of the Public?	
--------------------------------------	--

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	2/14/22
Departmental Element & Site	Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33), Integrated Joint Cybersecurity Coordination Center (iJC3) DOE Germantown Campus, Room CA-007
Name of Information System or IT Project	Ticketing and Automation System (TAAS) FedRAMP Package ID F1305072116
Exhibit Project UID	N/A
New PIA <input type="checkbox"/>	Update in light of new personnel tracking functionality.
Update <input checked="" type="checkbox"/>	

	Name, Title	Contact Information Phone, Email
System Owner	Robert Knisely iJC3 Manager Office of the Chief Information Officer (OCIO) Cybersecurity Operations (IM33) Integrated Joint Cybersecurity Coordination Center (iJC3)	301-903-0988 robert.kinsely@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson Privacy Management and Compliance Officer / DOE IM-42	202-287-5786 brooke.dickson@hq.doe.gov
Cyber Security Expert reviewing this	Paul Abulu (CTR) ISSO, iJC3	Office: 301-903-7701



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE I – PRIVACY NEEDS ASSESSMENT

document (e.g. ISSM, CSSM, ISSO, etc.)		
Person Completing this Document	Robert Knisely iJC3 Manager	301-903-0988 Robert.Knisely@hq.doe.gov
Purpose of Information System or IT Project	<p>The Integrated Joint Cybersecurity Coordination Center (iJC3) serves as the coordination and collaboration hub for cyber incidents, information sharing, and reporting for DOE’s enterprise cybersecurity program. iJC3 falls under the purview of the Chief Information Officer (OCIO). iJC3’s objective is to coordinate enterprise cybersecurity efforts, provide common tools, establish methodologies (to address cybersecurity events), and provide a centralized reporting framework for the Department. iJC3 regularly communicates with sites and contacts throughout the DOE. iJC3’s current ticketing system has become obsolete and has limited functionality. iJC3 purchased a ServiceNow solution that offers a superior platform and user experience. The result is the Ticketing and Automation System (TAAS), a cloud-based web portal which support iJC3 operations used to facilitate:</p> <ol style="list-style-type: none"> 1) Cybersecurity incident reporting from both internal (DOE) sources and to external recipients (Department of Homeland Security). Examples: loss/theft, phishing, impersonation spoofing; 2) Requests for service. Examples include account removal/request and site distribution list; 3) Requests for information; 4) Track personnel with sponsoring organization and clearance levels for Headquarters Security Officer (HSO) record keeping. Example: Individual names, clearance level, clearance status, and sponsoring organization. <p>TAAS will be accessible to all DOE employees and contractors who are able to authenticate via the OneID system. Standard end users will be able to access the system and report cybersecurity incidents and/or make requests for information or service. iJC3-designated cyber points of contact will have accounts in TAAS and, in addition to the above functionality, will be able to view all ticket information for their respective sites.</p> <p>TAAS is built on the FedRAMP-approved software-as-a-service (SaaS) ServiceNow platform. More specifically, iJC3 has implemented the Security Incident Response (SIR) application, which is a part of the larger Security Operations suite offering from ServiceNow.</p> <p>The HSO application spreadsheet resides in TAAS and is used to track personnel including name, sponsoring organization, and clearance level for HSO record keeping purposes. The HSO dashboard is responsible for tracking the status of current and new employee’s security clearance when they join the Department of Energy (DOE) organization. The data table is</p>	



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE I – PRIVACY NEEDS ASSESSMENT

	<p>used to record, edit/update, and show information about an employee’s security clearance level that was entered by the HSO administrator who has the same reporting rights from TaaS/SNOW.</p>
<p>Type of Information Collected or Maintained by the System:</p>	<ul style="list-style-type: none"> <input type="checkbox"/> SSN <input type="checkbox"/> Medical & Health Information <input type="checkbox"/> Financial Information <input type="checkbox"/> Clearance Information <input type="checkbox"/> Biometric Information <input type="checkbox"/> Mother’s Maiden Name <input type="checkbox"/> DoB, Place of Birth <input type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name, Phone, Address <input checked="" type="checkbox"/> Other – The information collected depends on the ticket type (Service Request, Request for Information, or Incident Report). <p>For <i>Service Requests:</i></p> <ol style="list-style-type: none"> 1. Service Request information (type and description); 2. Submitter contact information (name and email); 3. Reporting office information (program office; site; POC; email; name; phone); 4. Depending on service request type (beneficiary’s name and email). <p>Additionally, attachments <i>may</i> be added.</p> <p>For <i>Requests for Information:</i></p> <ol style="list-style-type: none"> 1. Submitter information (name and email); 2. Reporting office information (program office; site; POC; email; name; phone; description). <p>Additionally, attachments <i>may</i> be added.</p>



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE I – PRIVACY NEEDS ASSESSMENT

For ***Incident Reports*** (*Attrition, Impersonation Spoofing, Removable Media, Other, Phishing, Unknown, Loss or Theft, Improper Usage, and Web*):

1. Submitter’s name and work email address is collected at the site level on behalf of the site
2. Reporting office information (Program Office, site, POC, email, name, business phone)
3. Incident details (date and time of incident; internal tracking number; name, email, and phone number of impacted user; existing iJC3 ticked number (if applicable); confirmation of spillage event (Y or N); incident description; and confirmation of whether confidentiality, integrity, and/or availability of information systems has been affected (Y or N)
4. Functional impact information (functional impact definition; characterization of observed activity at its most severe level; # users impacted; # systems impacted; location (defined by levels 1-7) at which activity was observed)
5. Whether PII exists. (Y or N)
6. Impacted operating systems (name and version of impacted O/S); function of system affected
7. Informational impact (description of known informational impact from incident; confirmation of if incident is considered to be a breach that must be reported to Congress w/in 30 days in accordance w/ OMB guidance (Y or N); confirmation of if incident is considered to be a “major incident” per OMB guidance (Y or N)
8. Technical information (incident detection method; netflow (if available); CVE-ID (if available))
9. Indicators of compromise (email address; IP address; domain; port; protocol)
10. Recoverability / Mitigation (recoverability ability; details regarding recoverability)
11. Resolution (confirmation of readiness to close incident (Y or N); resolution details)

For ***Headquarters Security Officer (HSO) Request For Information (RFI)***

1. Allows approved user to track Individual Name, Sponsoring Organization, Clearance Level and Clearance Status.
2. Whether PII exists. (Y or N)

Additionally, attachments *may* be added.

Has there been any attempt to verify PII does not exist on the system?

DOE Order 206.1, Department of Energy Privacy Program, defines PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to

The system contains PII.



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE I – PRIVACY NEEDS ASSESSMENT

<i>distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.</i>	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	Yes (see above). Basic contact information will be collected from the submitter at the site level during initial reporting of an incident on behalf of the site. No additional PII will be intentionally collected or stored.
2. Is the information in identifiable form?	Yes.
3. Is the information about individual Members of the Public?	No.
4. Is the information about DOE or contractor employees?	<input checked="" type="checkbox"/> Federal Employees <input checked="" type="checkbox"/> Contractor Employees

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?	<ul style="list-style-type: none"> P.L. 106-65, "National Defense Authorization Act [Section 3212(d)], enacted October 1999. Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. Seq. Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C.
--	---



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE II – PII SYSTEMS & PROJECTS

- The Cybersecurity Information Sharing Act of 2015 (“CISA”), requires the Director of National Intelligence and the Departments of DHS, Defense, and Justice to develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threats.

In general, CISA authorizes the sharing of cyber threat indicators and defensive measures:

- For a “cybersecurity purpose,” defined to mean “the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.” Id. §102(4);
- Consisting of information that meets the definition of a “cyber threat indicator” or “defensive measures.” (See frequently asked question (FAQ) #7 for a discussion of “cyber threat indicators” and “defensive measures.”);
- Following the review and removal of any personal information of a specific person or information that identifies a specific person that the sharer knows is not directly related to a cyber threat. Id. § 104(d)(2); and
- In compliance with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicators or defensive measures.

CISA provides that, “notwithstanding any other provision of law, a non-federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-federal entity or the Federal Government a cyber threat indicator or defensive measure.” CISA, §104(c)(1) (emphasis added).

1. CONSENT

What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the

- 1) All visitors to the portal will see the following system use / warning banner, which clearly states that logging in is equivalent to providing consent. An individual, may, of course, choose not to log in to the system.

****WARNING**WARNING**WARNING**WARNING****

This is a Department of Energy (DOE) computer system. DOE computer



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE II – PII SYSTEMS & PROJECTS

<p>information (other than required or authorized uses)?</p>	<p>systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY.</p> <p>**WARNING**WARNING**WARNING**WARNING**</p> <p style="margin-left: 40px;">2) On several screens (when inside TAAS) users have the <i>option</i> to upload attachments (that would contain additional information). User uploads aren't mandatory.</p>
<p>2. CONTRACTS</p> <p>Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?</p>	<p>Yes, contractors are involved with the design, development, and maintenance of TAAS. Privacy Act compliance clauses are included in all contractor agreements. These require contractors to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and DOE requirements.</p>
<p>3. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>TAAS is expected to improve how privacy and data spillage incidents are communicated and resolved at DOE. The system is designed to improve communication and workflows between security resources throughout DOE. Additionally, the system's reporting and analytic capabilities may provide new insight into trends regarding DOE privacy incidents. The system's purpose and use are consistent with that of Incident Response and Security Coordination Teams.</p> <p>Additionally, TAAS is not a public-facing system. Even within the DOE community, its use will be restricted to only those who can authenticate via OneID.</p> <p>The only PII collected by TAAS includes administrative PII pertaining to contact information and clearance. In addition to the low sensitivity of the PII as well as the controls protecting it, PII is not indexed and cannot therefore be retrieved by unique identifier beyond very narrow administrative retrieval by a small number of privileged personnel.</p> <p>The significant privacy protection facilitated by TAAS outweighs the small</p>



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE II – PII SYSTEMS & PROJECTS

	<p>privacy risk posed by the system. TAAS provides a significant privacy net benefit in light of the low sensitivity administrative PII collected by the system weighed against the ability to protect privacy interests the system provides DOE.</p>
<p>4. SORNs How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>Deliberate, indexed retrieval of PII is not possible for general users. Access to HSO data is restricted to 3 members of the HSO team with appropriate security permissions who may retrieve administrative PII (e.g., name, organization, clearance level) for administrative (record keeping) purposes. General users cannot retrieve PII by unique identifier. Moreover, data accessible to the HSO team could not be searched against other data in the system.</p>
<p>5. SORNs Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>? If "Yes," provide name of SORN and location in the <i>Federal Register</i>.</p>	<p>See answer to Question 4. PII is not indexed and cannot therefore be retrieved by unique identifier beyond very narrow administrative retrieval by a small number of privileged personnel; a SORN is therefore not required.</p>
<p>6. SORNs If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>N/A</p>
DATA SOURCES	
<p>7. What are the sources of information about individuals in the information system or project?</p>	<ol style="list-style-type: none"> 1) OneID (https://oneid.yc.energy.gov/info/#/idm) and PIV cards will be used to authenticate. TAAS users will need to supply their own PIV card. 2) Once inside the system, a user can enter basic contact information about themselves or, if submitting a ticket on behalf of someone else, another individual.
<p>8. Will the information system derive new or metadata about an individual from the information collected?</p>	<p>No. TAAS will be collecting the types of data stated in Module 1. Every ticket needs to be associated with at least one person, but TAAS does not generate new data or metadata about individuals.</p>



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE II – PII SYSTEMS & PROJECTS

9. Are the data elements described in detail and documented?	Yes. They are described in the FIPS-199 Security Categorization.
DATA USE	
10. How will the PII be used?	<p>The system will contain professional contact information about a DOE federal, contractor or site, lab, plant, or power administration (“site”) employee who is reporting an incident, requesting access (to the system) or another iJC3 system, or requesting information. Such information may be retained as part of monitoring logs and files as part of iJC3 security policy.</p> <p>Access to HSO data is restricted to 3 members of the HSO team with appropriate security permissions who may retrieve administrative PII (e.g., name, organization, clearance level) for administrative (record keeping) purposes.</p>
11. If the system derives metadata, how will the new or metadata be used? Will the new or meta data be part of an individual’s record?	<p>N/A.</p> <p>Metadata (as in incident log data) related to network traffic events may be provided to TAAS in a service request or incident ticket for the purpose of incident response coordination and collaboration, but this metadata does not contain PII and the system does not derive metadata about individuals.</p>
12. With what other agencies or entities will an individual’s information be shared?	Only iJC3 personnel (including TAAS system admins) and site-designated cyber POCs will be able to see tickets that have been submitted by people other than themselves. More specifically, site-designated cyber POCs will only be able to see tickets concerning their respective organization. Some users will need to have visibility at the Program Office level.
REPORTS	
13. What kinds of reports are produced about individuals or contain an individual’s data?	<p>Per NIST SP 800-53 / 800-37, TAAS is required to follow a number of auditing controls. As a result, audit logs are generated. These contain information such as user actions (login time, etc.).</p> <p>Most site-designated cyber POCs will have the ability to generate reports detailing all tickets associated with only their site. Some users will need to be able to have visibility at the Program Office level (multiple sites), however. All other users will be unable to generate reports.</p>
14. What will be the use of these reports?	Audit logs will be used for the security and management of the system. iJC3 produces specific daily, weekly, and monthly operations reports. One example is the Executive Summary Incident Report. The iJC3 must also be



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE II – PII SYSTEMS & PROJECTS

	<p>able to generate situational reports. PII would not be collected, stored or searchable in these instances.</p> <p>Example: LANL’s designated cyber point of contact may call the iJC3 to report an Indicator of Compromise (present on their network). It would be extremely helpful for the iJC3 Analyst to be able to view LANL’s past (and any current) tickets (for incidents or IOCs). If an abnormal amount of problems are from one specific user, this information would be vital to properly assessing and resolving the problem. This type of capability is considered standard for security analysts to effectively perform their jobs.</p>
<p>15. Who will have access to these reports?</p>	<ol style="list-style-type: none"> 1) Authorized iJC3 system administrators and security personnel will have access to reports from all sites. 2) Site-designated cyber POCs will be able to view reports that cover only their (respective) sites. 3) Standard end users won’t have any report-viewing capability.

MONITORING

<p>16. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>TAAS is not a monitoring or identification system. Certain user actions are required to be logged.</p>
<p>17. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>Auditable user actions are logged, as TAAS is required to meet NIST-defined security controls. The system must be capable of auditing based on a risk assessment and mission/business needs in the DOE Program Cyber Security Policy (PCSP).</p> <p>Audit events include successful and unsuccessful logon, account creation / deletion, changes in account profiles, and error conditions.</p> <p>Further details can be found in the TAAS Security Plan.</p>
<p>18. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	<p>Yes. Access controls limit the users who can view audit logs.</p>

DATA MANAGEMENT & MAINTENANCE

<p>19. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.</p>	<p>There is an annual audit review where the ISSO and other stakeholders will review the details included in system audit records and determine if any more, less, or other details are required.</p>
---	---



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE II – PII SYSTEMS & PROJECTS

20. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A. There is only one production instance of TAAS, and it is hosted in the cloud. All system users, regardless of their geographic location, will be accessing this instance.
RECORDS MANAGEMENT	
21. Identify the record(s).	<ul style="list-style-type: none"> System audit records Cybersecurity incident reporting Requests for Cybersecurity services and information HSO personnel security tracking records
22. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	<p><input type="checkbox"/> Unscheduled <input checked="" type="checkbox"/> Scheduled <i>(cite NARA authority below)</i></p> <ul style="list-style-type: none"> GRS 3.2, item 020 - Computer security incident handling, reporting and follow-up records GRS 3.2, items 030 (or 031) - System access records GRS 5.6, item 190 - Index to the personnel security case files or GRS 5.6, item 010 - Security administrative records GRS 5.8, item 010 - Technical and administrative help desk operational records
23. Records Contact	Shannon Hughes, shannon.hughes@hq.doe.gov Dominick Littleton, dominick.littleton@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
24. What controls are in place to protect the data from unauthorized access, modification or use?	<p>As a system designed to further data security, TAAS employs a number of technical and administrative controls to protect data. The TAAS web portal itself can only be reached by DOE IP addresses. OneID further restricts login to those who have PIV cards.</p> <p>Upon login, privileges are determined by membership in role-based groups. To request privileged access, users are required to follow the iJC3 approval process.</p> <p>Implementation details are described in the system’s Security Plan.</p>
25. Who will have access to PII data?	iJC3 system administrators and site-designated POCs will have access to limited administrative PII associated with tickets.



PRIVACY IMPACT ASSESSMENT
 Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
 Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

MODULE II – PII SYSTEMS & PROJECTS

26. How is access to PII data determined?	Access to data in TAAS is restricted and role based.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	No. TAAS is a standalone system.
28. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	N/A.
29. Who is responsible for ensuring the authorized use of personal information?	The TAAS System Owner is responsible for ensuring authorized use of personal information. Access control lists are kept by iJC3 TAAS System Administrators and audited according to policy.

END OF MODULE II



PRIVACY IMPACT ASSESSMENT
Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
Integrated Joint Cybersecurity Center (iJC3)
Ticketing and Automation System (TAAS)

SIGNATURE PAGE		
	Signature	Date (If not digitally signed)
System Owner	<p>Robert Knisely</p> <hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/> <hr/>
Local Privacy Act Officer	<p>Brooke Dickson</p> <hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/> <hr/>
Ken Hunt Chief Privacy Officer	<p>William K. Hunt</p> <hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/> <hr/>