PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

DCSA Zero Trust Platform

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

12/19/2025

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

☐ From members of the general public

☐ From Federal employees

☒ from both members of the general public and Federal employees

☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

☒ New DoD Information System

☐ New Electronic Collection

☐ Existing DoD Information System

☐ Existing Electronic Collection

☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The DCSA Zero Trust Cloud Platform is a container for Okta, Zscaler, and CrowdStrike. Their descriptions are as follows:

Okta is a comprehensive identity and access management platform, hosted in the AWS IL5 Cloud environment, that helps organizations securely connect people to the right applications and resources at the right time. Key features of Okta include Single Sign-On (SSO) and Multi-Factor Authentication (MFA), which enhance security, improve user experience, and streamline IT operations.
Okta collects Personally Identifiable Information (PII) to manage user identities and secure access to systems. This can include data such as names, email addresses, phone numbers, and other personal identifiers. The PII collected by Okta may come from a variety of individuals, including potential or existing Federal employees and contractors who require access to the organization's systems and applications.

Zscaler is a cloud-based cybersecurity platform, hosted in the AWS GovCloud IL5 environment, designed to protect organizations and their data while allowing users, workloads, and devices to safely access applications and information from anywhere. Its primary purpose is to ensure that only authorized people and devices can access sensitive resources, while blocking harmful activities like hacking, malware, and phishing attacks. Zscaler works by acting as a gatekeeper for internet traffic and application access. When a user tries to access an application or website, Zscaler verifies if they are allowed to do so based on their identity and security rules. If everything meets the requirements, the user is granted access. If anything looks suspicious, access is blocked to prevent threats.
The system does not collect data entered on web forms such as SSN, address, DOB etc. Depending on the Mission Owner’s Zscaler configuration, Zscaler may process Personally Identifiable Information (PII) in the form of the organizational user's name and email address. This information is used to verify the identity of users and ensure that they are authorized to access specific applications and resources. The system tracks this data as part of its workflow to apply security measures, detect threats, and maintain a safe environment for users. The types of individuals whose data may be collected within the system include potential and existing Federal employees and contractors who need access to the organization’s applications and data.

CrowdStrike is a cybersecurity solution, hosted in AWS GovCloud IL5 environment, that helps organizations protect their computers, networks, and data from online threats like hacking, malware, and ransomware. It provides software that continuously monitors systems for suspicious activity, both prior to login and continuously thereafter, automatically responding to block or remove potential threats, ensuring sensitive information remains secure at all times. ex. When a laptop requests access to DCSA resources, CrowdStrike assigns a continuously evaluated Zero Trust (ZT) score, which indicates the device's security health. Based on this score, access to resources will either be granted or denied. CrowdStrike works by installing an agent on devices within an organization’s network, such as computers, servers, and mobile devices. This agent collects data about device usage, looking for unusual behaviors that might signal a cyberattack. If a threat is detected, CrowdStrike alerts the security team and can take action to stop the attack in real time.
How it uses PII: CrowdStrike might collect Personally Identifiable Information (PII) if a device is compromised. For example, tracking a user's identity (like an employee) can help understand the source of a threat. While CrowdStrike does not focus on collecting or storing PII, it

may capture basic information like to detect, analyze, and respond to security events.

Types of personal information:
- Usernames and email addresses.
- IP addresses
- Device identifiers.
- Activity data

Categories of individuals: CrowdStrike collects data about users within an organization, such as:
- Employees
- Contractors

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

These are the items these systems can search by and others are information that can be retrieved from the search. However, only privileged level users will be able to access the areas of these systems that contain this information.

Okta
1. Full Name: Used to identify the individual (e.g., John Doe).
2. Username or User ID: Unique identifiers for each user within the system.
3. Email Address: Used for user identification, authentication, notifications, and communication.
4. Phone Number: May be used for Multi-Factor Authentication (MFA), account recovery, or notifications.
5. Password: Encrypted for security purposes, used to authenticate users.
6. Security Question Answers: In some cases, answers to security questions are used to recover or verify accounts.
7. IP Address: The user’s IP address may be logged for security and auditing purposes, such as monitoring login attempts and detecting unusual activity.
8. Device Information: Device identifiers, including the type of device (e.g., mobile phone, laptop), operating system, and device ID.
9. Authentication Logs: Information about login times, successful and failed login attempts, IP address, and location of access.
10. Geolocation Data: Derived from the user’s IP address or other means to track the physical location during login attempts or activity.
11. Job Title or Role: In some configurations, job title or role within the organization may be collected to define user permissions and access levels.
12. Organization/Department Information: Information about the user's organizational affiliation to apply security policies, roles, and permissions.
13. Multi-Factor Authentication (MFA) Data: This could include temporary authentication codes sent via SMS, email, or authenticator apps.

Zscaler
1. User Identifiers:
- Email address
- Username or account ID

2. Contact Information:
- Phone numbers (in some cases)

3. Device Information:
- Device type (e.g., laptop, mobile phone, tablet)
- Device operating system and software
- Device ID or unique identifier

4. IP Address:
- User's public IP address from which they are accessing the network or application

5. Geolocation Data:
- Geographical location based on IP address (sometimes collected as part of threat detection or fraud prevention)

6. Authentication Data:
- Information related to login attempts, including authentication tokens or credentials
- Multi-factor authentication (MFA) information, if used

Crowdstrike
1. Usernames: The names of users logging into the system, typically tied to employee or contractor accounts.
2. Email addresses: These are used for identifying user accounts or for communication related to security events and alerts.
3. Device identifiers: Unique IDs associated with the devices being monitored (e.g., laptops, desktops, or mobile devices).
4. IP addresses: The public or internal IP addresses of devices being monitored, which can help identify the source or location of network traffic.
5. Authentication data: This can include information used to verify a user's identity, such as tokens or credentials related to the login process.

6. Session information: This may include data such as timestamps, session durations, and the specific actions taken by users on devices.
7. Geolocation data: Sometimes, IP addresses are used to determine the geographic location of devices, especially in the context of unusual or suspicious activity.
8. Behavioral data: Information about the actions users take on their devices (e.g., files accessed, applications used, websites visited) to detect potential threats or unauthorized access.

While CrowdStrike collects some of these data points for security purposes, it does not actively gather personal information beyond what is necessary for threat detection and response. The platform's primary goal is to protect systems from cyber threats and ensure the security of devices, networks, and data. It's important to note that PII collection is often specific to how an organization configures the CrowdStrike platform and what data is required for their security needs. The organization using CrowdStrike typically controls access to and use of the collected data, within the bounds of privacy laws and security policies

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes □ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

When accessing the network, the individual is provided the DoD Privacy and Consent Notice. They can object to collection if they decline to accept notice and choose not to access the network. If the individual accepts the notice and connects to our network, then their information is collected.

f. Do individuals have the opportunity to consent to the specific uses of their PII? □ Yes ☒ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Individuals cannot consent to the specific uses of their PII, however, these uses are outlined in SORN DoD 0015.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

□ Privacy Act Statement ☒ Privacy Advisory □ Not Applicable

Department of Defense Privacy and Consent Notice
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
At any time, the USG may inspect and seize data stored on this IS.
Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒	Within the DoD Component	Specify.	Security personnel responsible for the security of DCSA networks
□	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
□	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
□	State and Local Agencies	Specify.	
□	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
□	Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☐ Individuals

☒ Databases

☒ Existing DoD Information Systems

☒ Commercial Systems

☐ Other Federal Information Systems

National Background Investigation Services - Investigation Management (NBIS-IM)

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail

☐ Official Form (*Enter Form Number(s) in the box below)*

☐ In-Person Contact

☐ Paper

☐ Fax

☐ Telephone Interview

☒ Information Sharing - System to System

☒ Website/E-Form

☐ Other *(If Other, enter the information in the box below)*

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DoD 0015

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date.

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 3.2- Information System Security Records

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Computer security incident handling, reporting and follow-up records: Temporary. Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.

System access records: Systems requiring special accountability for access, Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

Cybersecurity logging records: Cybersecurity event logs, Temporary. Destroy when 30 months old. Longer retention is authorized for business use.

PKI transaction-specific records: Temporary. Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority (“internal housekeeping”) as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

10 U.S.C. 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 10 U.S.C. 2224, Defense Information Assurance Program; 10 U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities; 31 U.S.C. 902, Authority and functions of agency Chief Financial Officers; Homeland Security Presidential Directive (HSPD) 12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management; National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors; DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense; DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense; and DoD Instruction 8520.03, Identity Authentication for Information Systems.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

□ Yes ☒ No □ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections.”
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

The system does not actively solicit information from the public but, rather receive the information passively from the mission systems it provides authentication for. User information is derived from the mission systems at a minimal level to create an account for access to the required DCSA systems. All other information collected is done so pursuant to the "consent to monitoring" clause.