Privacy Impact Assessment

Abstract

The E-Government Act of 2002 requires that US Government agencies conduct and make public a privacy impact assessment (PIA) when "developing electronic projects that collect, maintain or disseminate information in identifiable form from or about the public." National security systems are not subject to the PIA requirement. At its discretion, however, the Office of the Director of National Intelligence (ODNI) conducts impact assessments to ensure that new business processes do not infringe privacy rights and civil liberties. This PIA is issued in accordance with that policy and has been reviewed and approved by the ODNI Civil Liberties Protection Officer.

CTIIC Organization and Operations

The Cyber Threat Intelligence Integration Center (CTIIC) was established pursuant to the Presidential Memorandum dated February 25, 2015, which directed the DNI to establish such a center under the authority conferred to him by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 to create national intelligence centers.

In the memorandum, the President assigned five responsibilities to CTIIC:

1. Provide integrated all-source analysis of intelligence related to foreign cyber threats or related to incidents affecting US national interests;
2. Support the National Cybersecurity and Communications Integration Center (NCCIC), the National Cyber Investigative Joint Task Force (NCIJTF), US Cyber Command (USCYBERCOM), and other relevant US Government entities by providing access to intelligence necessary to carry out their respective missions;
3. Oversee the development and implementation of intelligence-sharing capabilities (including systems, programs, policies, and standards) to enhance shared situational awareness of intelligence related to foreign cyber threats or related to cyber incidents affecting US national interests among the organizations referenced already;
4. Ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification possible for distribution to both US Government and US private sector entities through the mechanism described in section 4 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity); and
5. Facilitate and support interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to US national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

CTIIC Components

CTIIC personnel include ODNI permanent staff ("ODNI cadre"), detailees from other intelligence agencies, and contractors. CTIIC's leadership team is also multiagency and includes senior officials from the major US Government producers of cyber threat intelligence. Together, CTIIC personnel support the integration, analysis, and sharing of information related to foreign cyber threats or cyber incidents affecting US national interests to support decisionmaking.

- Most CTIIC personnel are all-source analysts with expertise in cyber threat actors and the tactics they employ. These personnel use critical thinking, analytic tradecraft, knowledge of Intelligence Community (IC) information sources and research methodologies, and strong communication skills to produce integrated analytic products.
- CTIIC also includes Interagency Coordination Officers who work with a broad set of departments and agencies to help develop "whole of government" options against cyber adversaries.
- CTIIC's Publications Team supports these activities by providing expertise in classification markings, editorial review, graphic design, and secure dissemination of intelligence products.

CTIIC Operations

CTIIC personnel support three main lines of effort to achieve CTIIC's mission.

Building Awareness: Awareness of our adversaries' threat activities is the first step in disrupting and mitigating their consequences. CTIIC builds this awareness by integrating the intelligence threat reporting with contextual information that tells the broader story. This work serves as a building block for trend analysis, makes cyber reporting accessible to nonspecialists, and highlights the threats' potential significance for decisionmakers. CTIIC analysts continually examine intelligence reporting to identify the most significant threats; gather contextual data by reaching out to other centers, departments, and agencies to get different perspectives and fill in the information gaps; and pull together information on what the US Government as a whole is doing in response.

Presidential Policy Directive (PPD) 41 on Cyber Incident Coordination names ODNI, through CTIIC, as one of three Federal lead agencies (with DHS and FBI) to coordinate the response to a significant cyber incident. CTIIC is the lead for intelligence support and related activities.

Integrating Analysis: CTIIC leads analysis of current and near-term cyber threats, collaborating with cyber and noncyber subject-matter experts to initiate and integrate IC analysis that considers adversaries' threat activity, intent, and motivations in a geopolitical context. In many cases, significant cyber incidents have occurred in conjunction with geopolitical tension and have been preceded by actions or statements that indicated the adversaries' intent. To identify likely perpetrators and targets of malicious cyber activity, CTIIC's analysts build broad IC expert communities representing all of the disciplines related to cyber threats—especially technical, regional, and strategic analysis.

Identifying Opportunities: CTIIC supports and facilitates whole-of-government options in response to cyber threats. This help provides decisionmakers with potential courses of action that reflect all instruments of national power. Before the US Government plans a cyber campaign, CTIIC provides analysis to help frame the "art of the possible" and establish a repeatable framework for presenting options to policymakers. This framework considers risk/benefit trade-offs; diplomatic, military, intelligence, economic, and other equities; and measures of progress and success.

To accomplish its mission, CTIIC has access to a broad range of open-source and federal information, including Top Secret, Secret, and Unclassified federal intelligence and law enforcement (LE) community systems, databases, reporting, and analysis.

CTIIC reviews federal and LE reporting for (i) timely and credible information about cyber threats, (ii) intelligence about individuals and groups intending to carry out malicious cyber activity against US national interests, and (iii) major events or circumstances that might influence the choice of defensive measures against potential malicious cyber activity. To that end, CTIIC reviews:

1. **Threat Reporting.** CTIIC reviews alerts, warnings, notifications, and updates of time-sensitive information related to malicious cyber activity against US national interests.
2. **Incident Reporting.** CTIIC reviews significant events or activities occurring at the international, national, state, and local levels to assess whether these events and activities have the potential to raise concern within the US Government about the potential for malicious cyber activity against the United States.
3. **Finished Intelligence.** CTIIC reviews IC strategic and foundational assessments concerning malicious cyber activity to the United States before and after dissemination.

Privacy Discussion

CTIIC receives information that has already been vetted by other agencies and therefore accesses very little personally identifiable information (PII). The PII that CTIIC does receive most likely consists of the names of companies and individuals and the e-mail addresses of cyber attack victims.

CTIIC processes mitigate the potential privacy impact of CTIIC operations. Several factors contribute to the potential impact on privacy, including the following:

- The inability of subjects to consent to the collection of their PII,
- The vulnerabilities arising from individual CTIIC members' having access to sensitive PII, and
- The potential dissemination of more PII than is relevant and necessary.

The First Line of PII Protection: The Impact Assessment Process

In part, CTIIC mitigates the potential impact by having an ongoing assessment of how the organization handles PII.

Limited Collection of PII

CTIIC does not task or perform collection activities—it has access only to evaluated intelligence from other federal entities as it relates to foreign cyber threats or cyber incidents affecting US national interests. The limited amount of PII that CTIIC receives is based on each source agency's legal, regulatory, or policy constraints.

Limited Use of PII

Based on CTIIC's authorities, CTIIC analysts may only access, query, or otherwise use received information—including PII—for a purpose related to foreign cyber intelligence. CTIIC's mandate is to integrate reporting and analysis of current and near-term foreign cyber threats and incidents. In support of this mission, CTIIC works with federal cyber centers and interagency partners to produce an integrated picture of threat intelligence, incidents, and response.

Limited Dissemination of PII

Under Executive Order 12333, Unites States Intelligence Activities, IC elements may collect, retain, and disseminate information concerning US persons in accordance with procedures established by the head of the IC element and approved by the Attorney General, in consultation with the ODNI. The ODNI and its components—including CTIIC—follow CIA's Attorney-General-approved procedures. Accordingly, CTIIC's dissemination of PII must comply with those procedures and any supplemental guidance issued by CTIIC. Generally speaking, this means CTIIC employees may disseminate PII within ODNI to
(a) employees who need to know the information in the course of their official duties and (b) other appropriate elements within the IC to allow recipients to determine whether the information relates to their responsibilities and can be retained by them.

CTIIC may not disseminate PII outside the IC unless it has been determined that the identity information is necessary to understand or assess the intelligence being disseminated and the dissemination is permitted by CIA procedures.

CTIIC's finished products are disseminated electronically, by one of two methods: (a) posting on IC-authorized websites or (b) by e-mail sent to the IC and a select group of other federal entities with significant cyber-related responsibilities.

Appropriate System Security

CTIIC operates within existing processes governing the production of cyber threat reporting, information, and intelligence at ODNI. In accordance with ODNI's Records Management retention schedule, CTIIC will retain the following in its local analytic files:

- Evaluated information accessed by CTIIC and used in support of CTIIC analysis or CTIIC products, and
- All products disseminated by CTIIC.

Note: CTIIC's existence and activities *do not* affect protocols for protecting federal systems otherwise accessible to CTIIC from outside intrusions.

Appropriately Trained Personnel

CTIIC personnel—whether ODNI cadre, detailees from other intelligence agencies, or contractors—are vetted against rigorous federal requirements. These include passing a Top Secret/Special Background Investigation, and having an active Top Secret//Sensitive Compartmented Information (TS//SCI) Clearance. All personnel also receive a comprehensive orientation from the CTIIC Civil Liberties and Privacy Officer on legal and security topics, including guidelines for PII protection and product dissemination.

No Focus on Individuals

At this time, CTIIC does not anticipate using PII in a manner that would trigger application of the Privacy Act, 5 USC 552a. CTIIC's interest focuses on threats, warnings, and incidents rather than on individuals. Therefore, CTIIC will not use elements of PII for US individuals to query collected information and will not create a system of records under the Privacy Act. In the event that CTIIC's mission broadens to focus on individual actors, CTIIC will publish a system-of-records notice as required by subsection 552a(e)(4) of the Act.