**Privacy Impact Assessment Update**
**for**

# EINSTEIN 3 - Accelerated ($E^3A$)

# DHS/PIA/NPPD-027(a)

# May 6, 2016


**Contact Point**
**Andy Ozment Assistant Secretary**
**Office of Cybersecurity & Communications**
**National Protection and Programs Directorate**
**(703) 235-5999**

**Reviewing Official**
**Karen L. Neuman**
**Chief Privacy Officer**
**Department of Homeland Security**
**(202) 343-1717**

# Abstract

The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) is conducting this Privacy Impact Assessment (PIA) Update to describe the addition of a new intrusion prevention security service, known as Web Content Filtering (WCF), to the EINSTEIN 3 Accelerated (E$^3$A) program. WCF provides protection at the application layer for web traffic by blocking access to suspicious websites, preventing malware from running on systems and networks, and detecting and blocking phishing attempts as well as malicious web content. This service will be added to the existing E$^3$A intrusion prevention security services that are already in place and are described in the original E$^3$A PIA published April 19, 2013.


# Overview

The Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C) continues to improve its ability to defend federal civilian Executive Branch department/agency (D/A) networks from cyber threats. DHS deployed EINSTEIN 3 Accelerated (E$^3$A) in 2013 to enhance the Federal Government's cybersecurity analysis, situational awareness, and security response. With E$^3$A, DHS is not only able to detect malicious traffic targeting the federal civilian Executive Branch D/A networks, but also able to prevent malicious traffic from harming those networks. It does so by delivering intrusion prevention capabilities as Managed Security Services (MSS) provided by Internet Service Providers (ISPs). Under the direction of DHS, ISPs administer intrusion prevention security services on network traffic entering and leaving federal civilian Executive Branch D/A networks.

The National Cybersecurity Protection System (NCPS)[1] includes an intrusion prevention capability, operationally known as EINSTEIN 3 Accelerated (E$^3$A), and is part of the integrated system that is used to defend the federal civilian Executive Branch Government information technology infrastructure from cyber threats. With E$^3$A, DHS is able to detect malicious traffic and take proactive measures to prevent it. The description of the program articulated in the April 2013 E$^3$A PIA remains unchanged and DHS continues to leverage MSS[2] provided by ISPs to administer intrusion prevention and threat-based decision making on network traffic entering or leaving federal civilian Executive Branch D/A networks.

All EINSTEIN operations (including E$^3$A and its Web Content Filtering (WCF) service) are carried out in a manner reasonably necessary to protect federal civilian Executive Branch D/A information and their respective information systems from a cybersecurity risk. As used in this

[1] The published EINSTEIN and other cyber related PIAs can be found at: http://www.dhs.gov/cybersecurity-and-privacy.
[2] MSS is a model by which the Government articulates the objectives and service levels expected; ISPs then determine how and at what cost those services are delivered.

document, the term "cybersecurity risk" (A) means threats to, and vulnerabilities of, information or information systems as well as any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism, and (B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement. DHS will retain, use, and disclose information obtained through the operation of EINSTEIN only to protect information and information systems from cybersecurity risks. DHS will retain information obtained through EINSTEIN no longer than reasonably necessary for the purpose of protecting federal civilian Executive Branch D/A information and their respective information systems from a cybersecurity risk.

## Reason for the PIA Update

The DHS National Protection and Programs Directorate (NPPD) is conducting this Privacy Impact Assessment (PIA) Update to describe the addition of a new intrusion prevention security service, known as WCF, which provides protection at the application layer for web traffic by blocking access to suspicious websites, preventing malware from running on systems and networks, and detecting and blocking phishing attempts as well as malicious web content. This service will be added to the existing E$^3$A intrusion prevention security services that are already in place and are described in the original E$^3$A PIA published April 19, 2013.

**Web Content Filtering**

E$^3$A allows DHS to better detect, respond to, and appropriately defend against, known or suspected cyber threats identified within the network traffic it monitors. The initial implementation of E$^3$A involved two intrusion prevention security services: Domain Name Server (DNS) Sinkholing[3] and Email Filtering.[4] DHS will add further protections to federal civilian Executive Branch D/As with the addition of WCF. WCF will provide protection for web traffic[5] by blocking access to certain websites that are known to be, or include, malicious content (malware). In addition, WCF will prevent malware from suspicious websites from running on federal civilian Executive Branch D/A systems and networks. Finally, WCF will also detect and/or block phishing attempts as well as the undesirable content that may be included in those attempts.

[3] DNS Sinkholing protects against the use of Domain Name Server (DNS) as a means to establish communication with compromised hosts or to distribute malware. This capability is achieved by redirecting user traffic that matches known cyber threat indicators to a safe host to (1) prevent connection to a malicious host and (2) collect data on the attempted malicious connection.

[4] Email filtering protects against the use of malicious file attachments and embedded links in email content by preventing emails that match known cyber threat indicators from reaching their intended destination and collecting information on malicious activity.

[5] E.g., Hyper Text Transfer Protocol (HTTP) and HTTP Secure (HTTP/S), which includes the content of web sessions.

WCF categorizes web-based suspicious traffic, to include all URL/URIs and the content of web sessions,[6] which allows system operators to specifically allow or disallow certain types of content that is known to be, or includes, malicious content (malware). WCF service can be configured to alert or block on traffic based on the applicable high-confidence cyber threat indicators and commercial signature development technology (used by the ISP) to allow DHS to block and alert against web-based traffic. This will permit traffic suspected by DHS as malicious as well as customer-specific cybersecurity risk protection requirements to alert or block on specific types of traffic. WCF provides this service via a web proxy between the client and the web server it is attempting to access. The proxy will perform the actions such as redirect, prevent, and/or alert on attempted access to certain (i.e., malicious) web content that matches a DHS cyber threat indicator that may look for a specific URL/URI or webpage content.

WCF capabilities also include in-line Secure Socket Layer (SSL) decryption;[7] malware detection; and advanced analytics. WCF SSL provides visibility into specific types of organizational traffic (including web content) that has been encrypted, for the purpose of protecting that traffic from malicious activity that would otherwise remain hidden by traversing encrypted channels. The capability decrypts web traffic of D/As participating in the E$^3$A[8] WCF capability for the purpose of detecting and preventing malicious web content on the D/A network. DHS is not interested in the behavior of individuals; decryption is focused on web communications, not communications between individuals. DHS does not use this capability to investigate the behavior or private content of individuals. Malware detection is an inherent part of operating WCF. WCF protects specific federal civilian Executive Branch D/A traffic by using Government-furnished cyber threat indicators to detect malicious activity. Advanced analytics in this context refers to behavior-based (heuristic) threat indicators to identify how a cyber threat or any of the anomalous characteristics of a cyber threat, a computer system, or the data behaves.

WCF will use applicable high-confidence cyber threat indicators created using processes similar to those already deployed for E$^3$A's DNS and Email Filtering. DHS and the specific D/A at which WCF is activated will receive notifications when an alert is generated from a match against a WCF indicator, allowing DHS and the D/A to take appropriate action(s) as needed.

As with other E$^3$A intrusion prevention security services, WCF will not monitor internal agency traffic, nor will it monitor network traffic that is wholly on the Internet. E$^3$A only monitors the limited network traffic that passes to or from a federal civilian Executive Branch D/A network and the Internet in relation to the applicable cyber threat indicators identifying malicious activity.

[6] Uniform Resource Identifier (URI) is the information (string of characters) used to identify the resource on the World Wide Web. The Uniform Resource Locator (URL) is typically the Web address and most commonly used type URI.
[7] DHS will decrypt web sessions between EINSTEIN users and the web content they are accessing. This is limited to the encryption of communications between servers to identify potentially malicious web sites.
[8] See below for identified privacy risks and possible mitigations.

Based on the evolution of the cyber threat, DHS may add additional security services to E$^3$A, and will continue to monitor any changes to potential collection and use of Personally Identifiable Information (PII).

# Privacy Impact Analysis

In each of the sections below, DHS has taken into consideration how the updates may have changed the risks and impacts based on the fair information principles. In some cases there are no changes and the PIA Update is indicated as such.

### Authorities and Other Requirements

EINSTEIN is carried out pursuant to Section 230 of the Homeland Security Act, as added by the Consolidated Appropriations Act, 2016.[9] Authorities relevant to DHS's broader cybersecurity mission include the Federal Information Security Modernization Act of 2014[10] and other provisions of title II of the Homeland Security Act, as amended.

Consistent with the previously published PIA, the Privacy Act does not apply to information regarding known or suspected cyber threats, which includes information related to WCF. The Privacy Act does apply when PII may be used as an identifier for authorized users granted access to the NCPS or E$^3$A (such as a username or a Government-issued email address). The DHS General Information Technology Access Account Records Systems (GITAARS), Privacy Act System of Records Notice (SORN)[11] permits DHS to collect and maintain general contact and other related information used to grant access to employees, contractors, and other individuals to the DHS information technology resources, including NCPS.

As was documented in the 2013 E$^3$A PIA, each ISP is required to provide DHS with a system security plan (SSP) that specifically documents its intrusion prevention security services implementation. As part of the DHS intrusion prevention security services security risk assessment process, the SSP will be updated by each ISP to include WCF, and will be reviewed and approved by CS&C prior to the deployment of WCF as a new intrusion prevention security service solution.

Information is not being collected or solicited directly from the public; therefore, the Paperwork Reduction Act (PRA) does not apply with the addition of WCF as a service to E$^3$A.

There are no new privacy risks to authority or purpose specification with the addition of WCF to E$^3$A.

[9] Pub. L. No. 114-113, Division N, section 223 (6 U.S.C. § 151).
[10] 44 U.S.C. § 3551 et seq.
[11] DHS/ALL-004 General Information Technology Access Account Records Systems (GITAARS) SORN (November 27, 2012, 77 FR 70792).

## Characterization of the Information

Through E$^3$A, DHS observes network and Internet traffic travelling to or from federal civilian Executive Branch D/A networks by delivering intrusion prevention capabilities as an MSS provided by ISPs. With the introduction of WCF, DHS is now better able to detect malicious web-based traffic targeting federal civilian Executive Branch D/A networks and prevent that same malicious traffic from harming those networks. WCF categorizes web-based suspicious traffic, to include all URL/URIs, which allows system operators to specifically allow or disallow certain types of content.[12] WCF services can be configured to alert and/or block on traffic based on the applicable high-confidence cyber threat indicators and commercial signature development technology (by the ISP) to allow DHS to block and/or alert against web-based traffic. This will permit traffic suspected by DHS as malicious as well as customer-specific protection requirements to alert/block on specific types of traffic. WCF provides this service via a web proxy between the client and the web server it is attempting to access.[13] The proxy will perform the actions such as redirect, prevent, or alert on attempted access to certain web content that matches a DHS cyber threat indicator that may look for a specific URL/URI or webpage content.

The introduction and use of WCF services does not change the amount or type of information that is identified or collected for E$^3$A.

## Uses of the Information

There are no changes to DHS use of information in the E$^3$A intrusion prevention program. DHS will use information obtained through operation of EINSTEIN only to protect information and information systems from cybersecurity risks. The addition of WCF to E$^3$A intrusion prevention security services does not change the use of the information collected, as outlined in the previous PIA. WCF will add an additional service to the existing intrusion prevention security capabilities that monitors traffic travelling to or from federal civilian Executive Branch D/A networks, in real time, for specific pre-defined cyber threats. When a specific threat is detected, based on existing DNS Sinkholing and Email Filtering services, and now WCF, the deployed E$^3$A

[12] Threat categories area an industry standard and are part of the standard product offerings provided by available commercial off-the-shelf products that can be used by the provider. These categories include: File Transfer Categories (i.e., File Storage/Sharing; Peer-to-Peer (P2P); Software Downloads); Security Concern Categories (i.e., Hacking; Piracy/Copyright Concerns; Computer/Information Security; Placeholders; Potentially Unwanted Software; Remote Access Tools; Spam; Suspicious); and Security Threat Categories (i.e., Phishing; Proxy Avoidance; Malicious Outbound Traffic / Botnets; Malicious Sources/Malnets).

[13] Although the system does log attempted accesses to sites identified as malicious or bad, end user information is not provided or collected. The collection and use of log information is addressed in the original E$^3$A PIA; see relevant risks/mitigations re: analysis, quarantine, storage, or maintenance of more data than is necessary to address cybersecurity threats.

countermeasures may automatically block packets transiting to or from agency networks to counter the cyber threats.

**Privacy Risk:** There is a risk that PII obtained through the decryption of D/A web traffic by the E$^3$A WCF capability will be used inappropriately.

**Mitigation:** CS&C has specific guidelines and procedures that govern the handling and safeguarding of PII that may be collected for NCPS and EINSTEIN activities, which includes any PII that may be obtained through the decryption of D/A web traffic by the E$^3$A WCF capability. These processes are managed through contract requirements, Rules of Behavior for system access, information handling guidelines and standard operating procedures (SOP), and privacy training.

Access to the NCPS and E$^3$A is restricted to government and contractor staff with demonstrated need for access, and such access must be approved by the supervisor as well as the CS&C Information System Security Manager (ISSM). Authorized users (i.e., NCPS system administrators and CS&C cybersecurity analysts) must sign Rules of Behavior that identify the need to protect PII prior to gaining access. Once access is granted, DHS logs and monitors all NCPS user actions to ensure compliance with system requirements, including the proper handling, safeguarding, and use of PII encountered for NCPS and EINSTEIN activities such as when PII is obtained during the decryption of D/A web traffic for the E$^3$A WCF capability. Failure to abide by the Rules of Behavior may result in disciplinary measures and potential termination of employment.

CS&C personnel (i.e., CS&C cybersecurity analysts, NCPS system administrators, and information assurance personnel) receive privacy training upon hire, annual refresher Security Education and Awareness Training (SEAT), as well as annual Role Based Cyber Privacy Training on specific CS&C procedures for handling and safeguarding PII.

ISPs providing E$^3$A intrusion prevention security services receive copies of established CS&C guidelines and SOPs regarding the handling and minimization of PII and the identification of sensitive information that may contain PII. As contractors to CS&C, the ISPs are required to conduct their activities in accordance with DHS requirements, including privacy training. Failure to meet these guidelines will be addressed through appropriate corrective action as defined by contract.

**Notice**

There are no changes from the previous PIA that affect the notice provided to D/A users, and what is already noted by privacy policies on an agency's website. The addition of WCF does not change the MOA requirements with DHS by the D/A with respect to privacy notices and logon banners. Similarly, this PIA Update, along with the original 2013 E$^3$A PIA and the NCPS PIA

serve as a general notice to individuals that network traffic, including web-based traffic, flowing to or from federal civilian Executive Branch D/A may be collected for computer security purposes.

There are no new privacy risks to notice identified with the addition of WCF to E$^3$A.

**Data Retention by the project**

DHS will retain information obtained through EINSTIEIN only to protect information and information systems from cybersecurity risks. And DHS will retain information obtained through EINSTEIN no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk. A records retention schedule for the National Cybersecurity Protection System (NCPS) (Record Schedule #DAA-0563-2013-0008) was approved on January 12, 2015.[14]

**Information Sharing**

Within the restriction that DHS will disclose information obtained through EINSTEIN only to protect information and information systems from cybersecurity risks, and as described in previous cybersecurity compliance documents, information collected, analyzed, or otherwise obtained by CS&C in connection with known or suspected cybersecurity threats or cyber incidents may be disclosed as part of their work products in furtherance of the DHS cybersecurity mission to protect federal information systems from cybersecurity threats and to mitigate against such threats, or respond to a cyber incident in accordance with the cybersecurity information handling policies and guidelines and relevant law.

The addition of WCF to E$^3$A intrusion prevention security services does not change the sharing of such cyber threat information, nor does it generate any new privacy risks to information sharing.

**Redress**

Information regarding known or suspected cyber threats collected from federal D/As, state, local, and tribal governments, industry, the general public, and international partners and collected by the NCPS and EINSTEIN, is not based on data that identifies an individual but on the security event that triggered the alert. The addition of WCF to E$^3$A intrusion prevention security services follows the same procedures identified and published in the E$^3$A and NCPS PIAs and does not

[14] The link to the approved NARA Record Schedule DAA-0563-2013-0008 is included here: http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0008_sf115.pdf; and

change the opportunities identified in the previously published cybersecurity PIAs. ISPs use E$^3$A to analyze traffic and create reports based on indicators, not by PII. The security event that triggered the alert is how data is retrieved, stored, and reported.

**Privacy Risk:** A risk remains that individuals are unable to seek redress for data associated with a known or suspected cyber threat.

**Mitigation:** Additional redress procedures beyond those described in the previously published E$^3$A PIA or the National Cybersecurity Protection System (NCPS) PIA are not available because information collected as part of the NCPS and EINSTEIN is not based on data that identifies an individual but instead on the security event that triggered the alert. ISPs use E$^3$A to analyze traffic and create reports based on indicators, not by PII. The security event that triggered the alert is how data is retrieved, stored, and reported. As such, there is no information about an individual that can be used to access the cybersecurity threat or event(s).

### Auditing and Accountability

There are no changes to the auditing and accountability requirements from previously published cybersecurity PIAs.

## Responsible Official

Andy Ozment
Assistant Secretary, Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

## Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security