Request for Records Disposition Authority

Records Schedule Number	DAA-0563-2013-0008
Schedule Status	Approved
Agency or Establishment	Department of Homeland Security
Record Group / Scheduling Group	General Records of the Department of Homeland Security
Records Schedule applies to	Major Subdivsion
Major Subdivision	National Protection and Programs Directorate (NPPD)
Schedule Subject	National Cybersecurity Protection System (NCPS)
Internal agency concurrences will be provided	No

Background Information

The National Cybersecurity Protection System (NCPS) is an integrated system of intrusion detection, analytics, intrusion prevention, and information sharing capabilities. These capabilities provide a technological foundation for defending the federal civilian government's information technology infrastructure against advanced cyber threats. NCPS, which is delivered through a combination of hardware, software, and managed security services, advances the Department of Homeland Security (DHS) responsibilities for meeting the cybersecurity mission requirements as delineated in the Comprehensive National Cybersecurity Initiative (CNCI).

NCPS capabilities of information sharing, analysis, and detection and prevention rely on tight collaboration and integration with cross-Federal stakeholders in order to support the defense of the underlying networks. The analysis of the network monitoring traffic data provides valuable cyber incident information and generates situational awareness and decision support data that is used by incident response teams, government critical infrastructure organizations, and national leadership. Response teams use the information to thwart cyber-attacks, to point to the origins of the attack, and respond to the attacks in a timely manner. Executive managers and national leaders make valuable decisions on what policies and resources are needed in order to respond to and prevent the current and future attacks.

NCPS capabilities span five broad technology areas:

•DETECTION: Enables DHS to detect malicious activity as it transits in and out of federal civilian information technology (IT) networks.

•ANALYTICS: Provides DHS analysts with the ability to compile and analyze information about cyber activity and inform Federal, state and local government agencies, private sector partners, infrastructure owners and operators, and the public about current and potential cybersecurity threats and vulnerabilities.

•INFORMATION SHARING: Establishes a flexible set of capabilities, implemented at multiple classification levels that will allow for the rapid exchange of cyber threat and cyber incident information among DHS cyber security analysts and their cybersecurity partners.

•PREVENTION: Advances the protection of federal civilian departments and agencies by providing active network defense capabilities and the ability to prevent and limit malicious activities from penetrating federal networks and systems.

•CORE INFRASTRUCTURE: Includes the classified and unclassified Mission Operating Environment and communications infrastructure, including operations services, development and testing, and incident management systems.

Item Count

Number of Total Disposition Items	Number of Permanent Disposition Items	Number of Temporary Disposition Items	Number of Withdrawn Disposition Items
6	0	6	0

GAO Approval

Outline of Records Schedule Items for DAA-0563-2013-0008

Sequence Number	
1	Master File/ Data
1.1	Core Infrastructure (MOE, E3A MOE, Incident Management System, Dev/Test E nvironment) Disposition Authority Number: DAA-0563-2013-0008-0001
1.2	Intrusion Detection (EINSTEIN 1, EINSTEIN 2, pDNS) Disposition Authority Number: DAA-0563-2013-0008-0002
1.3	Intrusion Prevention (E3A) Disposition Authority Number: DAA-0563-2013-0008-0003
1.4	Analysis (PCAP, SIEM, EADB, AMAC, Digital Media Analysis Environment) Disposition Authority Number: DAA-0563-2013-0008-0004
1.5	Information Sharing (CyberScope, US-CERT.gov Website and US-CERT Portal, CIR/CIAP) Disposition Authority Number: DAA-0563-2013-0008-0005
2	Output
2.1	Analysis and reports on data which may be relayed to other components within C S&C or to systems in organizations other than the NCPS. Disposition Authority Number: DAA-0563-2013-0008-0006

Records Schedule Items

Sequence Number	
1	Master File/ Data
1.1	Core Infrastructure (MOE, E3A MOE, Incident Management System, Dev/Test Environment)
	Disposition Authority Number: DAA-0563-2013-0008-0001
	Data collected includes: •Individual's contact information and the nature of the concern. •Suspicious files, spam, and other potential cyber threats via an email network, exclusively used within the MOE •Synthetic cyber threat data
	Final Disposition: Temporary
	Item Status: Active
	Is this item media neutral?: Yes
	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?: Yes
	Do any of the records covered by this item exist as structured electronic data?: Yes
	Disposition Instruction
	Cutoff Instruction: Cutoff at date of receipt.
	Retention Period: Destroy or delete when 3 years old or when no longer needed for agency business, whichever is later.
	Additional Information
	GAO Approval: Not Required
1.2	Intrusion Detection (EINSTEIN 1, EINSTEIN 2, pDNS)
	Disposition Authority Number: DAA-0563-2013-0008-0002
	Data collected includes: •Netflow records •Information relating to DNS queries that is captured by collecting the requests and responses from the DNS servers •Alerts when a pre-defined specific cyber threat is detected and provides the US-CERT with increased insight into the nature of that activity •Custom signatures based upon known or suspected cyber threats
	Final Disposition: Temporary
	Item Status: Active
	Is this item media neutral?: Yes

	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
	Do any of the records covered by this item exist as structured electronic data?	Yes
	Disposition Instruction	
	Cutoff Instruction	Cutoff at date of receipt.
	Retention Period	Destroy or delete when 3 years old or when no longer needed for agency business, whichever is later.
	Additional Information	
	GAO Approval	Not Required
1.3	Intrusion Prevention (E3A)	
	Disposition Authority Number	DAA-0563-2013-0008-0003
	•Indicators of known or suspected cyber threats •Indicator reports	
	Final Disposition	Temporary
	Item Status	Active
	Is this item media neutral?	Yes
	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
	Do any of the records covered by this item exist as structured electronic data?	Yes
	Disposition Instruction	
	Cutoff Instruction	Cutoff at date of receipt.
	Retention Period	Destroy or delete when 3 years old or when no longer needed for agency business, whichever is later.
	Additional Information	
	GAO Approval	Not Required
1.4	Analysis (PCAP, SIEM, EADB, AMAC, Digital Media Analysis Environment)	
	Disposition Authority Number	DAA-0563-2013-0008-0004
	•Metadata derived from the PCAP analysis may contain email addresses and IP addresses. •Database for supporting commercially available visualization	

and analytical tools that allow US-CERT analysts to quickly visualize relevant relationships between disparate data and indicators of interest by presenting drill-down views of data with patterns, trends, series, and associations to analyze seemingly unrelated data •Digital Media Analysis environment is a segregated, closed, computer network system that is used to conduct timely investigative analysis of digital devices and their storage mediums in support of US-CERT staff and constituent •The AMAC, receives information about computer security vulnerabilities and threats in the form of actual malicious code submitted to US-CERT.

Final Disposition	Temporary
Item Status	Active
Is this item media neutral?	Yes
Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
Do any of the records covered by this item exist as structured electronic data?	Yes

Disposition Instruction

Cutoff Instruction	Cutoff on date of receipt.
Retention Period	Destroy or delete when 3 years old or when no longer needed for agency business, whichever is later.

Additional Information

GAO Approval	Not Required

1.5 Information Sharing (CyberScope, US-CERT.gov Website and US-CERT Portal, CIR/CIAP)

Disposition Authority Number DAA-0563-2013-0008-0005

•D/A FISMA reporting data •The US-CERT.gov website allows for the dissemination of general information to the public about US-CERT and its activities, as well as information pertinent to the discipline of cybersecurity. Additionally, the website is the primary means for members of the public to interact with US-CERT, request information, and report incidents (4 forms – CSET, ICSJWG, NCAS, and Report form) •CIR/CIAP is a common repository for sightings and indicators.

Final Disposition	Temporary
Item Status	Active
Is this item media neutral?	Yes

	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
	Do any of the records covered by this item exist as structured electronic data?	Yes
	Disposition Instruction	
	Cutoff Instruction	Cutoff on date of receipt.
	Retention Period	Destroy or delete when 3 years old or when no longer needed for agency business, whichever is later.
	Additional Information	
	GAO Approval	Not Required
2	Output	
2.1	Analysis and reports on data which may be relayed to other components within CS&C or to systems in organizations other than the NCPS.	
	Disposition Authority Number	DAA-0563-2013-0008-0006
	•Analyze data quality and utility; •Analyze data to establish trends and patterns for future enforcement actions; and •Other analytic functions in support of DHS cybersecurity and other mission related purposes.	
	Final Disposition	Temporary
	Item Status	Active
	Is this item media neutral?	Yes
	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
	Do any of the records covered by this item exist as structured electronic data?	Yes
	Disposition Instruction	
	Cutoff Instruction	Cutoff on date of receipt or creation.
	Retention Period	Destroy or delete when 5 years old or when no longer needed for agency business, whichever is later.
	Additional Information	
	GAO Approval	Not Required

Agency Certification

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal in this schedule are not now needed for the business of the agency or will not be needed after the retention periods specified.

Signatory Information

Date	Action	By	Title	Organization
09/16/2013	Return to Submitter	Tammy Hudson	Acting Records Officer	CIO - ESDO
09/24/2013	Certify	Tammy Hudson	Acting Records Officer	CIO - ESDO
12/22/2014	Submit for Concurrence	Erin Cayce	Appraiser	National Archives and Records Administration - Records Management Services
12/29/2014	Concur	Margaret Hawkins	Director of Records Management Services	National Records Management Program - Records Management Services
01/08/2015	Concur	Laurence Brewer	Director, National Records Management Program	National Archives and Records Administration - National Records Management Program
01/12/2015	Approve	David Ferriero	Archivist of the United States	Office of the Archivist - Office of the Archivist