U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	FireEye Email Threat Prevention (ETP) Software as a Service (SaaS)			
Office/Directorate:	EXIT			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Bobby Sanderson, ISSO, EXIT, x7832			
System Owner: (Name, title, organization and ext.)	Patrick Manley, CISO, EXIT, x7734			
System Manager: (Name, title, organization and ext.)	Bobby Sanderson, ISSO, EXIT, x2021			
B. APPROVING OFFICIALS	Signature	Approve	Disapprove	Date
System Owner Patrick Manley				
Privacy Advocate Bobby Sanderson, EXIT	BOBBY SANDERSON Digitally signed by BOBBY SANDERSON DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=BOBBY SANDERSON, 0.9.2342.19200300.100.1.1=61001001866635 Date: 2016.10.12 09:01:20 -04'00' Bobby Sanderson, ISSO	X		
Chief Information Security Officer Patrick Manley, EXIT	PATRICK MANLEY Digitally signed by PATRICK MANLEY DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=PATRICK MANLEY, 0.9.2342.19200300.100.1.1=61001000000929 Date: 2016.10.12 08:17:47 -04'00' Patrick Manley, CISO	X		
Senior Agency Official for Privacy Mary James, EXIT System of Record? _____Yes __X_No	MARY JAMES Digitally signed by MARY JAMES DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=MARY JAMES, 0.9.2342.19200300.100.1.1=6100100 0016516 Date: 2016.10.13 13:46:57 -04'00' Mary James, Deputy CIO			
Reviewing Official: James Rolfes, EXIT	JAMES ROLFES Digitally signed by JAMES ROLFES DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=JAMES ROLFES, 0.9.2342.19200300.100.1.1=61001001116382 Date: 2016.10.18 13:11:27 -04'00' James Rolfes, CIO	X		
C. SYSTEM APPLICATION/GENERAL INFORMATION				
1. Does this system contain any personal information about individuals? (If there is NO information collected, maintained, or used that is identifiable to the individual, the remainder of PIA does not have to be completed.)	Yes.			
2. Is this an electronic system?	Yes			
D. DATA IN THE SYSTEM				
1. What categories of individuals are	Public, Employees, and Contractors			

covered in the system? (public, employees, contractors)	
2. Generally describe what data/information will be collected in the system.	eMails entering and leaving CPSC will be captured and analyzed in FireEye's ETP cloud environment for malicious content and malware.
3. Is the source of the information from the individual or is it taken from another source? If not directly from individual, then what other source?	The emails originate from individuals inside and outside of CPSC.
4. How will data be checked for completeness?	The email servers at CPSC are configured to forward only inbound and outbound mail to/from CPSC. The Exchange servers will only process messages whose content conforms to RFC5321 and RFC5322 standards.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	The email is collected and forwarded real-time.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	See http://www.rfc-base.org/rfc-5321.html and http://www.rfc-base.org/rfc-5322.html
E. ATTRIBUTES OF THE DATA	
1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed?	The FireEye ETP Cloud-based system is necessary to supplement the protection of the agency against malware, advanced persistent threats (ATP's), and malicious content embedded in emails. ETP accomplishes this by forwarding the emails to FireEye's team of malware experts for analysis..
2. For electronic systems, if the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Explain.	ETP cloud offering will only store data that is connected to malicious code. The data will only be accessed by those analyst authorized access during the course of malware investigations after an alert or issue is identified. FireEye complies with NIST 800-88 destruction requirements.
3. How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.	Emails are retrieved by redirecting their destination through CPSC's Exchange 2013 servers to the FireEye ETP cloud. No personal identifiers are used in this redirection process.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	None. The collection and analysis of this data is permissible under Homeland Security Act of 2002 (6 U.S.C. §§ 101 et seq., esp. § 230 of the Homeland Security Act); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §§ 3551-3558); Presidential Policy Directive-21; National Security Presidential Directive-54/Homeland Security Presidential Directive-23; and the Federal Cybersecurity Enhancement Act of 2015 (Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Division N, section 221-229, esp. 223.)
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	eMails are only retained for the initial analysis period and are not stored. Malicious code associated with malware is retained until no longer relevant to the investigation of the malware itself. The following retention periods are identified for email containing potential malicious attachments or content: Quarantine: 15 days Advanced Threats: 90 days

	Email Logs: 30 days User Activity Tracking: 30 days
2. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are procedures documented?	Data is removed from FireEye's servers once analysis is completed. Please see FireEye Terms of Service: https://www.fireeye.com/company/legal.html#exhibitb4
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	Identify – yes, by email address only. The system does not provide the capability to locate or monitor individuals, or provide additional identification other than a user's email address.
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	Access to the ETP portal is restricted to only those with authorized accounts. These accounts require registration through FireEye customer support with authorization from the CPSC point of contact.
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No it is not.
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	N/A
G. ACCESS TO DATA	
1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	FireEye's ETP analysts and CPSC's EXIT team that requires access, (currently 5 people – two in TSNE and three in IT Security).
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	FireEye's ETP practices identified in the service agreement. https://www.fireeye.com/company/legal.html#exhibitb4
3. Who is responsible for assuring proper use of the data?	CPSC and FireEye, Inc.
4. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? Are contractors involved in the collection of the data? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?	FireEye, as contracted by CPSC for services provide maintenance and administration of the ETP cloud solution. Privacy clauses are contained in the CPSC contract.
5. Do other systems share data or have access to the data in the system? If yes, explain. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?	No other systems share or have access to the data in FireEye's ETP cloud.

6. Will other agencies share data or have access to the data in this system? If yes, how will the data be used by the other agency?	No
7. Will any of the personally identifiable information be accessed remotely or physically removed?	No.