U.S. Consumer Product Safety Commission PRIVACY IMPACT ASSESSMENT				
Name of Project:	Defender (Arcmail)			
Office/Directorate:	EXIT			
A. CONTACT INFORMATION				
Person completing PIA: (Name, title, organization and ext.)	Youssef Takhssaiti, IT Specialist (INFOSEC), EXIT, x7852			
System Owner: (Name, title, organization and ext.)	Terry Bard, Director, EXIT, x7700			
System Manager: (Name, title, organization and ext.)	Denis Suski, Branch Chief, EXIT, x6724			
B. APPROVING OFFICIALS	**Signature**	**Approve**	**Disapprove**	**Date**
System Owner Terry Bard, Director	TERRY E. BARD DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=TERRY BARD, 0.9.2342.19200300.100.1.1=6100100000925 Date: 2018.03.28 06:55:53 -04'00' Terry Bard, Director			
Privacy Advocate	YOUSSEF TAKHSSAITI Digitally signed by YOUSSEF TAKHSSAITI DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=YOUSSEF TAKHSSAITI, 0.9.2342.19200300.100.1.1=6100100309579 Date: 2018.05.01 10:32:27 -04'00'			
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: 2018.04.20 10:23:52 -04'00' Patrick Manley, CISO	X		4/20/18
Senior Agency Official for Privacy James Rolfes, EXIT **System of Record?** _____**Yes** __X__**No**	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: 2018.04.30 17:26:09 -04'00' James Rolfes, CIO	X		4/30/18
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: 2018.04.30 17:26:42 -04'00' James Rolfes, CIO	X		4/30/18
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 covered in the system? (public, employees, contractors)	Employees, contractors, and public.
2. Generally describe what data/information will be collected in the system.	Defender is an application used for archiving of all CPSC email, so anything that comes through email will be collected in the system.
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?	CPSC email.
4. How will data be checked for completeness?	N/A
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	System receives copies of emails sent from exchange for archival.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	All e-mails are stored locally on the Defender appliance.
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?	As part of CPSC's policy for e-mail retention, we are holding all inbound/outbound and internal messages indefinitely. This system handles the capture and storage of all e-mails.
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.	System requires external access only for maintenance and troubleshooting. SSL connection link is managed by Network Engineering and only available on an as needed basis.
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.	The data can be retrieved using any number of methods, including date, subject, To: From:, etc. – anything that is in an e-mail message can be searched on.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	None
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	The data is held indefinitely
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?	N/A
3. For electronic systems, will this system provide the capability to identify, locate, and monitor	No

individuals? If yes, explain.	
4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?	N/A
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No
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).	Select admin staff in ITTS, security staff in ITSO, Legal contractors in GC
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	The primary controls to prevent data misuse are restricting access to the system, ensuring all staff have taken the mandatory IT Security and Privacy Awareness training, and performing periodic reviews of searches performed.
3. Who is responsible for assuring proper use of the data?	The system owner will ensure EXIT administrators handle the data properly. The OGC COR is responsible for handling extracted data that is used for legal cases. EXIT has no insight into how and where they use that data
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?	The system is maintained by TSNE administrators. The data in Defender is collected directly from Microsoft Exchange but is retrievable by two contractors in OGC. A privacy clause is included in the purchase order.
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?	The only systems that share data are the Exchange e-mail servers. These servers are actually the feed for the data, all e-mails are journaled by the Exchange servers and this is how they are stored in the Defender appliance.
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?	The Dept. of justice (DOJ) will have indirect access to the information in Defender. The CPSC OGC contractors run searches for relevant data supporting legal actions being taken by the Commission. These legal actions often involve the DOJ.
7. Will any of the personally identifiable information be accessed remotely or physically removed?	Yes. Defender users on VDI have the capability to run searches while they are working remotely. As stated in question 6, data exported from Defender is shared with the DOJ and possibly opposing council in active legal cases.