United States
Consumer Product Safety Commission

Privacy Threat Analysis (PTA)/Privacy Impact Assessment (PIA)	
Name of Application/System:	Kevin Mitnick Security Awareness Training (KMSAT) + PhishER [KnowBe4]
Office/Directorate of System Owners:	Office of Information and Technology Services (EXIT), Information Technology Security Office (ITSO)
Office/Directorate of Business Owners:	EXIT, ITSO
Date:	March 19, 2024
A. Contact Information	
Person Completing PTA/PIA: (Name, title, organization)	Caitlyn Borghi, Chief Privacy Officer, EXIT
System Owner: (Name, title, organization)	Khalid Al-hassan, Chief Information Security Officer (CISO), EXIT
System Manager/Technical POC: (Name, title, organization)	Kenneth Grossman, Information Technology Security Operations Chief, EXIT
B. Approving Officials	
KHALID NUMAN AL-HASSAN System Owner	Digitally signed by KHALID NUMAN AL-HASSAN Date: 2024.04.24 16:15:50 -04'00'
CAITLYN BORGHI Chief Privacy Officer (CPO)	Digitally signed by CAITLYN BORGHI Date: 2024.04.23 15:42:00 -04'00'
KHALID NUMAN AL-HASSAN Chief Information Security Officer (CISO)	Digitally signed by KHALID NUMAN AL-HASSAN Date: 2024.04.24 16:11:29 -04'00'
ABIOYE MOSHEIM OYEWOLE Assistant General Counsel for Freedom of Information Act (FOIA), Records, and Privacy	Digitally signed by ABIOYE MOSHEIM OYEWOLE Date: 2024.05.03 15:10:51 -04'00'
 Senior Agency Official for Privacy (SAOP)	Digitally signed by BRYAN BURNETT DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=BRYAN BURNETT, 0.9.2342.19200300.100.1.1=61001000009719 Date: 2024.05.30 22:02:15 -04'00'

C. System of Records Notice	
1. Will the system or application maintain records that contain information about individuals? (Yes or No)	Yes.
2. Will the system or application allow records to be retrieved by an individual's name or by some identifying number, symbol, or other identifier assigned to the individual? (Yes or No)	Yes.
3. Will the records maintained by the system or application be considered a new collection of records? (Yes or No)	Yes.
If the answers to Questions 1 and 2 are yes and you do not currently have a System of Records Notice (SORN), one will be required.	
D. Privacy Threshold Analysis (PTA)	
4. Will the information system or application be used to collect, store, or transmit personally identifiable information (PII)? (Yes or No)	Yes.
5. Has a Privacy Impact Assessment (PIA) ever been performed for the information system or application? (Yes or No)	No.
6. Is there a Privacy Act System of Records Notice (SORN) for this information system or application? (Yes or No)	Yes.
If any of the answers to Questions 4 through 6 are "Yes" then complete the Privacy Impact Assessment (PIA) section (F) of this document. If the answers to Questions 4 through 6 are all "No" then a PIA is not needed. Complete section E below, sign form, and return to the Chief Privacy Officer.	
E. Omission of a Privacy Impact Assessment	
7. Briefly describe the information system or application and provide a supporting statement that explains why a PIA is not needed.	Not applicable.

F. Privacy Impact Assessment (PIA)	
8. Generally describe the type of information that will be collected, stored, or transmitted.	Kevin Mitnick Security Awareness Training (KMSAT) + PhishER [KnowBe4] is a privacy and security awareness training and phishing platform CPSC will use to support its privacy and security role-based training efforts and conduct regular phishing exercises. CPSC is required by OMB Circular A-130, *Managing Information as a Strategic Resource,* to provide advanced, role-based training to information system users and employees and contractors with assigned security and privacy roles and responsibilities. CPSC is required by the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and* Organizations, to provide training on recognizing and reporting potential and actual instances of social engineering and social mining; CPSC does this through annual phishing exercises. Employees and contractors' names, email addresses, and manager names will be uploaded to KnowBe4 from CPSC's email directory. CPSC will use this information to assign employees and contractors security and privacy training, track whether their training has been completed, and track employees and contractors' engagement with phishing exercises.
9. What categories of individuals are covered in the system? (For example, public, employees, contractors)	This system covers CPSC employees and contractors.
10. Is the personally identifiable information (PII) collected verified for accuracy? Why or why not?	Individuals are added and removed from CPSC's email directory when they join and leave CPSC. Updates, like changes in name, title, or organization, may occur on an as-needed basis. The names of individuals to be assigned training are verified with their managers on an annual basis.
11. Is the PII current? How is this determined?	Yes, the PII is current, as the names of individuals to be assigned training are verified with their managers on an annual basis.
12. Who will be responsible for protecting the privacy of the individuals whose PII is collected, maintained, or shared in the system? Have policies and/or	ITSO staff members and KnowBe4's CISO/Data Protection Officer and Vice President of Data Protection are responsible for protecting the privacy of the CPSC employees and contractors whose information is shared with and maintained in KnowBe4. ITSO is developing a privacy and security training plan that documents responsibilities for the role-based training process.

procedures been established for this responsibility and accountability?	KnowBe4's privacy responsibilities are listed in KnowBe4's Privacy Program document.
13. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?	Employees and contractors are able to contact the CPSC Service Desk to have their information in the email directory corrected or amended if it is incorrect.
14. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?	Information in the email directory is taken directly from employees and contractors. Employees and contractors' managers provide information on which of their staff have significant privacy and security roles and responsibilities.
15. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Employees and contractors do not have the opportunity to decline to provide information or consent to how their information is used. All CPSC employees and contractors are required to participate in and complete mandatory security and privacy trainings and exercises.
16. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII.	For role-based training, KnowBe4 will pull information from CPSC's email directory in order to assign individuals training. For phishing exercises, KnowBe4 will be granted access to CPSC's email directory and directly deliver phishing exercise-related messages to individuals' inboxes. KnowBe4 also connects to Datadog, KnowBe4's third-party audit logging service. This connection is necessary to produce application, system, and audit trail logs. Logs are retained for 30 days.
17. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-	KnowBe4 is a software-as-a-service (SaaS) platform, so KnowBe4 staff designed and perform maintenance on the platform. All KnowBe4 employees are required to sign Confidentiality and Non-Disclosure Agreements.

Disclosure Agreement (NDA) been developed for contractors who work on the system?	
18. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines?	The records in this system are covered under General Records Schedule Number DAA-GRS-2016-0014-0003. The records in the system are temporary; they should be destroyed when superseded, 3 years old, or 1 year after employee separation, whichever comes first. In KnowBe4, active production data, like account and associated data, are permanently deleted after termination and 18 months of account inactivity. For backup data and audit trails, backups are stored for 1 year and audit trails are stored for 3 years.
19. What are the procedures for disposition of PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed? (For example, shredding, degaussing, overwriting)	Information related to role-based training and phishing exercises stored on CPSC's SharePoint site will be deleted when ITSO no longer needs that information, adhering to the records schedule outlined in Question 18. Data is deleted in KnowBe4 via cryptographic erasure through an automated process.
20. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	This system operates under OPM SORN GOVT-1, General Employee Records.
21. Who will have access to the data in the system? (For example, contractors, managers, system administrators, developers, other)	ITSO staff will have access to the information in KnowBe4 in order to track training progress and analyze results of phishing exercises. Certain KnowBe4 administrators, users, developers, and contractors may have access to information on a need-to-know basis in order to provide CPSC services.
22. What controls are in place to prevent unauthorized access to the data?	Lists of employees to be assigned role-based training are stored in ITSO's SharePoint site where access is restricted to only those individuals with a need-to-know. KnowBe4 grants its employees access based on the principle of least privilege and need-to-know.

23. What controls are in place to prevent the misuse of PII by those having access?	ITSO staff are required to take security and privacy awareness training and sign a Rules of Behavior document upon joining CPSC and annually thereafter. KnowBe4 provides training to their staff based on their position and responsibilities before they are granted access to the information system. KnowBe4 employees are also required to complete security and privacy training annually. KnowBe4 grants its employees access based on the principle of least privilege and need-to-know. All access is monitored via audit log alerts and review to ensure those employees with access are not abusing it for purposes unrelated to their role. All KnowBe4 employees are required to sign Confidentiality and Non-Disclosure Agreements.
24. Is access to the PII being monitored, tracked, or recorded?	Yes, all access to PII is monitored, tracked, or recorded in KnowBe4's audit logging system. Lists of employees to be assigned role-based training are stored in ITSO's SharePoint site where access to documents is recorded.
25. For CPSC support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval?	ITSO, and some EXIT, staff will only have access to PII if they are responsible for operationalizing the CPSC role-based training and phishing exercise program or ensuring compliance with CPSC's program requirements. Access to PII in SharePoint will only be given to individuals within ITSO and EXIT who need to view the information. KnowBe4 grants its employees access based on the principle of least privilege and business need-to-know. All access is documented and monitored to ensure those with access are leveraging it for purposes related to their role. KnowBe4 leverages an Amazon Web Services (AWS) account management policy which determines what access individuals may have from administrator/developer roles.
26. What third-party organizations will have access to the PII? Who establishes criteria for what PII can be shared?	KnowBe4 uses AWS for its infrastructure; AWS is FedRAMP Moderate Authorized. KnowBe4's third-party audit logging service, Datadog, will have access to PII on a strict and temporary basis; Datadog is also FedRAMP authorized. KnowBe4 leverages ZenDesk for their customer support ticketing platform; as a result, ZenDesk will have access to ticket requesters' email address.
27. What CPSC personnel roles will have access to PII fields?	Certain KnowBe4 administrators, users, developers, and contractors may have access to information on a need-to-know basis in order to provide CPSC services.

(For example, users, managers, system administrators, developers, contractors, other)	ITSO staff will have access to PII in KnowBe4 as well.
28. Will any of the PII be accessed remotely or physically removed?	Lists of individuals who have not completed required training may be pulled from KnowBe4 and shared with EXIT leadership, individuals' managers, and other relevant KnowBe4 or CPSC staff in order to maintain compliance with CPSC requirements.