



**Privacy and Civil Liberties Impact Assessment (PCLIA)  
for the  
KnowBe4**

**Publication Date: 09-24-2024**

**Reviewing Official  
Bureau Privacy and Civil Library Officer**

---

# BUREAU OF ENGRAVING AND PRINTING

## Risk Level

This PCLIA is for a "major information system."

**The estimated number of individuals whose PII is maintained in the system is 1,000 - 9,999**

## Section 1: Introduction

PCLIAs are required for all systems and projects that collect, maintain, or disseminate [personally identifiable information](#) (PII). The system owner completed this assessment pursuant to Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget (OMB) Memorandum 0322, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before: (1) developing or procuring information technology (IT) systems or projects that collect, maintain or disseminate [PII](#) from or about members of the public, or (2) initiating a new collection of information that: (a) will be collected, maintained, or disseminated using [IT](#); and (b) includes any [PII](#) permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons (not including agencies, instrumentalities, or employees of the federal government).

It is the policy of the Department of the Treasury ("Treasury" or "Department") and its Bureaus to conduct a PCLIA when PII is maintained in a system or by a project. This PCLIA provides the following information regarding the system or project: (1) an overview of its purpose and functions; (2) a description of the information collected; (3) a description of the how information is maintained, used, and shared; (4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and (5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

## Section 2: System Overview

### Section 2.1: System Description and Purpose

1. The *Office of Critical Infrastructure and IT Security (OCIITS)* that own(s) or is funding the system, technology, pilot, rule, program, or other collection (hereinafter referred to as the "system") is conducting this PCLIA for the *KnowBe4* The program is conducting a PCLIA for this system for the first time.

2. The main purpose of this *KnowBe4* is to help the program meet its mission by *The KnowBe4 is Major Application*. *KnowBe4* is a provider of an integrated security awareness training and simulated phishing platform that is used by more than 24,000 organizations worldwide. Founded by data and IT security expert Stu Sjouwerman, with backing from Elephant Partners and Goldman Sachs Growth Equity, *KnowBe4* helps organizations address the human element of security by raising awareness of ransomware, CEO fraud, and other social engineering tactics through a new-school approach to security awareness training. Kevin Mitnick, internationally recognized computer-security expert and *KnowBe4's* Chief Hacking Officer, helped design *KnowBe4's* training based on his documented social engineering tactics. Thousands of organizations leverage *KnowBe4's* platform to train their workforce to make smarter security decisions and create a human firewall as an effective last line of defense. *KnowBe4's* Kevin Mitnick Security Awareness Training and Simulated Phishing platform (KMSAT) has approximately 25,000 customers. The platform is designed to provide users with a platform to better manage IT security problems of social engineering, spear-phishing, and ransomware attacks. . This system also allows the program to *The KnowBe4 is Major Application*. *KnowBe4* is a provider of an integrated security awareness training and simulated phishing platform that is used by more than 24,000 organizations worldwide. Founded by data and IT security expert Stu Sjouwerman, with backing from Elephant Partners and Goldman Sachs Growth Equity, *KnowBe4* helps organizations address the human element of security by raising awareness of ransomware, CEO fraud, and other social engineering tactics through a new-school approach to security awareness training. Kevin Mitnick, internationally recognized computer-security expert and *KnowBe4's* Chief Hacking Officer, helped design *KnowBe4's* training based on his documented social engineering tactics. Thousands of organizations leverage *KnowBe4's* platform to train their workforce to make smarter security decisions and create a human firewall as an effective last line of defense. *KnowBe4's* Kevin Mitnick Security Awareness Training and Simulated Phishing platform (KMSAT) has approximately 25,000 customers. The platform is designed to provide users with a platform to better manage IT security problems of social engineering, spear-phishing, and ransomware attacks. The KMSAT platform provides users self-service enrollment, and both pre-and post-training phishing security tests that show the percentage of end-users that are Phish-prone. *KnowBe4's* random Phishing Security Tests provide several remedial options in the event an employee falls for a simulated phishing attack.
3. The system is comprised of the following components: *KnowBe4 Cloud Phishing Platform (KMSAT)* .
4. The *Office of Critical Infrastructure and IT Security (OCIITS)* maintains personally identifiable information (PII) in the following system components: *KnowBe4 Cloud Phishing Platform (KMSAT)*
5. The *Office of Critical Infrastructure and IT Security (OCIITS)* collects/receives PII maintained in the system from:
  - a. N/A - *KnowBe4* obtains information on BEP employees and contractors from Active Directory and does not collect any PII directly from the individual.
  - b. *KnowBe4* obtains information on BEP employees and contractors from Active Directory and does not collect any PII directly from the individual
6. The *Office of Critical Infrastructure and IT Security (OCIITS)* uses the information in the system to: *KnowBe4* utilizes the information to conduct simulated phishing attacks, and improving user awareness of potential threats. This allows BEP to track who is susceptible to phishing attempts. *KnowBe4* utilizes user information to generate reports for administrators and auditors that helps provide insight to training completion, user performance, and helping BEP to meet compliance requirements.
7. The *Office of Critical Infrastructure and IT Security (OCIITS)* discloses the information in the system to the extent required by the Freedom of Information Act and as allowed by the Privacy Act of 1974 (including the routine uses in the applicable SORN: N/A

8. The *Office of Critical Infrastructure and IT Security (OCIITS)* identified the following privacy risks during collection, use, and disclosure: The program office did not identify any privacy risks for the PII in the system.
9. The *Office of Critical Infrastructure and IT Security (OCIITS)* has taken the following steps/implemented the following controls to protect the PII in the system during the collection, use, and disclosure: KnowBe4 collects PII that is necessary for the intended purpose to minimize data, and encrypts PII at rest and in transit to protect it from unauthorized access, and ensure that any disclosure is in line with legal requirements or other relevant data protection laws.

## Section 2.2: Authority to Collect

Federal agencies must have proper authority before initiating a collection of information. The authority is sometimes granted by a specific statute, by Executive order (EO) of the President or other authority. The following specific authorities authorize KnowBe4 to collect information:

- Public Law No. 113-283 (Federal Information Security Modernization Act of 2014)

The information may also be collected pursuant to a more general requirement or authority. All Treasury systems and projects derive general authority to collect information from:

- 31 U.S.C. 321 – General authorities of the Secretary establish the mission of the Department of the Treasury
- 5 U.S.C. 301 – Department regulations for the operations of the department, conduct of employees, distribution and performance of its business, the custody, use, and preservation of its records, papers, and property.

## Section 2.3: Privacy Act Applicability; SORN Requirement

Under certain circumstances, federal agencies are allowed to exempt a system of records from certain provisions in the Privacy Act. This means that, with respect to information systems and papers files that maintain records in that system of records, the agency will not be required to comply with the requirements in Privacy Act provisions that are properly exempted. If this system or project contains records covered by the Privacy Act, the applicable Privacy Act system of records notice(s) (SORNs) (there may be more than one) that cover the records in this system or project must list the exemptions claimed for the system of records (it will typically say: “*Exemptions Claimed for the System*” or words to that effect).

### Section 2.3(a)

- The system does not retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual. A SORN is not required with respect to the records in this system.

## Section 3: Information Collection Section

### 3.1: Relevant and Necessary The Privacy Act

requires “each agency that maintains a system of records [to] maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.” 5 U.S.C. § 552a (e)(1). It allows federal agencies to exempt records from certain requirements (including the relevant and necessary requirement) under certain conditions. 5 U.S.C. §552a (k). The proposed exemption must be described in a Notice of Proposed Rulemaking (“NPRM”). In the context

of the Privacy Act, the purpose of the NPRM is to give the public notice of a Privacy Act exemption claimed for a system of records and solicit public opinion on the proposed exemption. After addressing any public concerns raised in response to the NPRM, the agency must issue a Final Rule.

It is possible for some, but not all, of the records maintained in the system or by the project to be exempted from the Privacy Act through the NPRM/Final Rule process.

### ***Section 3.1(a) Exemption Claimed from this Requirement?***

- The PII maintained in this system or by this project is not exempt from 5 U.S.C. § 552a(e)(1), the Privacy Act's requirement that an agency maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.

### ***Section 3.1(b) Continuously Assessing Relevance and Necessity***

- With respect to PII *currently* maintained (as of the time this PCLIA is being done) in the system, the PII limited to only that which is relevant and necessary to meet the system's or project's mission requirements. During the PCLIA process, the system always undergoes a review to ensure the continuing relevance and necessity of the PII in the system.

### **Section 3.2: PII and/or information types or groupings**

The list below represent the types of information maintained in the system or by the project that are relevant and necessary for the information system or project to fulfill its mission. PII identified below is used by the system or project to fulfill the purpose stated in Section 2.2 above– Authority to Collect.

**Biographical/general information**

**Other information**

**Identifying numbers assigned to individuals**

**Specific Information/File Types**

**Audit Log and Security Monitoring Information**

**Medical/Emergency Information Regarding Individuals**

**Biometrics/Distinguishing Features/Characteristics of Individuals**

**Identifying numbers for sole proprietors (including business information)**

### **Section 3.3: Sources from which PII is obtained**

Focusing on the context in which the data was collected and used (i.e., why it is collected and how it is used), list **ALL** sources from which PII is collected/received and stored in the system or used in the project

**Members of the Public**

Other: BEP Federal contractors and interns.

### **Current Federal Employees, Interns, and Detailees**

Current Federal employees providing information in their capacity as federal employees;

## **Section 3.4: Privacy and/or civil liberties risks related to collection**

When Federal agencies request information from an individual that will be maintained in a [system of records](#), they must inform the individual of the following: “(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the [routine uses](#) which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on [the individual], if any, of not providing all or any part of the requested information.” 5 U.S.C § 522a(e)(3). This is commonly called a Privacy Act Statement.

The OMB Guidelines also note that subsection (e)(3) is applicable to both written and oral (i.e., interview) solicitations of personal information. Therefore, even if a federal employee or contractor has a fixed list of questions that they orally ask the individual in order to collect their information, this requirement applies.

### **Section 3.4(a) Collection Directly from the Individual to whom the PII pertains**

- None of the PII in the system was collected directly from an individual to whom it pertains: KnowBe4 obtains information on BEP employees and contractors from Active Directory and does not collect any PII directly from the individual.

### **Section 3.4(b) Privacy Act Statements**

- None of the PII in the system was collected directly from the individuals to whom it pertains. Therefore, a Privacy Act Statement is not required.

### **Section 3.4(c) Use of Full Social Security Numbers**

Treasury is committed to eliminating unnecessary collection, use, and display of full Social Security numbers ('SSN') and redacting, truncating, and anonymizing SSNs in systems and documents to limit their accessibility to individuals who do not have a need to access the full SSN in order to perform their official duties. Moreover, the Privacy Act provides that: 'It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.' Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. Id. at § 7(a)(2)(A)-(B).



### **Section 3.4(d) Justification for collection and use of full Social Security Numbers**

- N/A No full SSNs are maintained in the system. Explain if any portion of the SSN short of the full 9 digits is used in the system: SSN is not collected

### **Section 3.4(e) Controls implemented to limit access to and or improper disclosure of full Social Security Numbers**

### **Section 3.4(f) Denial of rights, benefits, or privileges for refusing to disclose Social Security Number**

- N/A No SSNs are maintained in the system or by the project.

### **Section 3.4(g) Records describing how individuals exercise First Amendment rights**

The Privacy Act requires that Federal agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

- N/A. The system *does not* maintain information describing how an individual exercises their rights guaranteed by the First Amendment.

## **Section 4: Maintenance, use, and sharing of the information**

### **Section 4.1: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared when it is used to make determinations about individuals**

The Privacy Act and Treasury policy require that Treasury bureaus and offices take additional care when collecting and maintaining information about individuals when it will be used to make determinations about those individuals (e.g., whether they will receive a federal benefit). This includes collecting information directly from the individual where practicable and ensuring that the information is accurate, relevant, timely and complete to assure fairness to the individual when making a determination about them. This section addresses the controls/protections put in place to address these issues.

The [Privacy Act](#) requires that Federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C § 552a(e)(5). If a particular [system of records](#) meets certain requirements (including the [NPRM](#) process defined in Section 3.1 above), an agency may exempt the [system of records](#) (or a portion of the records) from this requirement.

Exemptions may be found at the bottom of the relevant SORN next to the heading: “*Exemptions Claimed for this System.*”

#### **Section 4.1(a) Exemption from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act**

- *None* of the information maintained in the system that is part of a system of records is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act.

#### **Section 4.1(b) Protections in place despite exemption from the accuracy, relevance, timeliness, and completeness requirements**

- *None* of the information maintained in the system that is part of a system of records is exempt.

#### **Section 4.1(c) Collecting information directly from the individual when using it to make adverse determinations about them.**

Section 552a(e)(2) of the Privacy Act requires that Federal agencies that maintain records in a system of records are required to collect information to the greatest extent practicable directly from the individual when the information about them may result in adverse determinations about their rights, benefits, and privileges under Federal programs. Agencies may exempt a system of records from this requirement under certain circumstances and if certain conditions are met.

#### **Section 4.1(d) Additional controls designed to ensure accuracy, completeness, timeliness and fairness to individuals in making adverse determinations**

##### **1. *Administrative Controls***

Individuals about whom information is collected are given the following opportunities to amend/correct/update their information to ensure it is accurate, timely and complete to the extent reasonably necessary to assure fairness when it is used to make a determination about them:

- The PII collected for use in the system is NOT used to make adverse determinations about an individual's rights, benefits, and privileges under federal programs.

##### **2. *Technical Controls***

- No additional technical controls are available to ensure accuracy, relevance, timeliness and completeness.

#### **Section 4.2: Data-Mining**

As required by Section 804 of the [Implementing Recommendation of the 9/11 Commission Act of 2007](#) (“9-11 Commission Act”), Treasury reports annually to Congress on its data mining activities. For a comprehensive overview of Treasury’s data mining activities, please review the Department’s Annual Privacy Act and Data Mining reports available at: <http://www.treasury.gov/privacy/annual-reports>.

#### **Section 4.2(a) Is the PII maintained in the system used to conduct data-mining**

- The information maintained in this system or by this project *is not* used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act. Therefore, no privacy or civil liberties issues were identified in responding to this question.

#### **Section 4.3: Computer Matching**

The Computer Matching and Privacy Protection Act (CMPPA) of 1988 amended the [Privacy Act](#) by imposing additional requirements when Privacy Act systems of records are used in computer matching programs.

Pursuant to the CMPPA, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll [systems of records](#) or a system of federal personnel or payroll records with non-federal records. This type of matching program may be conducted for any purpose. The second type of matching program involves the computerized comparison of two or more automated [systems of records](#) or a [system of records](#) with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. *See* 5 U.S.C. § 522a(a)(8). Matching programs must be conducted pursuant to a matching agreement between the source (the agency providing the records) and recipient agency (the agency that receives and uses the records to make determinations). The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

#### **Section 4.3(a) Records in the system used in a computer matching program**

- The information maintained in the system *is* part of a Privacy Act system of records, but *is not* used as part of a matching program.

#### **Section 4.3(b) Is there a matching agreement?**

- N/A

#### **Section 4.3(c) What procedures are followed before adverse action is taken against an individual who is the subject of a matching agreement search?**

- N/A

## **Section 4.4: Information sharing with external (i.e., outside BEP) organizations and individuals**

### **Section 4.4(a) PII shared with/disclosed to agencies, organizations or individuals outside BEP**

- PII maintained in the system is *not* shared with agencies, organizations, or individuals external to Treasury.

### **Section 4.4(b) Accounting of Disclosures**

An accounting of disclosures is a log of all external (outside Treasury) disclosures of records made from a system of records that has *not* been exempted from this accounting requirement. This log must either be maintained regularly or be capable of assembly in a reasonable amount of time after an individual makes a request. Certain system of records may be exempted from releasing an accounting of disclosures (e.g., in law enforcement investigations).

### **Section 4.4(c) Making the Accounting of Disclosures Available**

- The records are not maintained in a system of records subject to the Privacy Act so an accounting is *not* required.

### **Section 4.4(d) Obtaining Consent Prior to New Disclosures Not Authorized by the Privacy Act Records**

in a system of records subject to the Privacy Act may not be disclosed by 'any means of communication to any person or to another agency' without the prior written request or consent of the individuals to whom the records pertain. 5 U.S.C. Sec. 552a(b). However, the Act also sets forth twelve exceptions to this general restriction. These 12 exceptions may be viewed at:

<https://www.justice.gov/usam/eousa-resource-manual-139-routine-uses-and-exemptions>. Unless one of these 12 exceptions applies, the individual to whom a record pertains must provide their consent, where feasible and appropriate, before their records may be disclosed to anyone who is not listed in one of the 12 exceptions. One of these 12 exceptions also allows agencies to include in a notice published in the Federal Register, a list of routine uses. Routine uses are disclosures outside the agency that are compatible with the purpose for which the records were collected.

### **Section 4.4(e) Obtaining Prior Written Consent**

- If a situation arises where disclosure (written, oral, electronic, or mechanical) must be made to anyone outside of the BEP who is not listed in one of the 12 exceptions in the Privacy Act (including the published routine uses), the individual's prior written consent will be obtained where feasible and appropriate.

## **Section 5: Compliance with federal information management requirements**

### **Section 5.1: The Paperwork Reduction act**

The [PRA](#) requires OMB approval before a Federal agency may collect standardized data from 10 or more respondents within a 12-month period. OMB also requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the [PRA](#), a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

#### **Section 5.1(a)**

- The system involves a new collection of information in identifiable form for 10 or more persons from outside the federal government.

### **Section 5.2: Records Management - NARA/Federal Records Act Requirements**

Records retention schedules determine the maximum amount of time necessary to retain information in order to meet the needs of the project or system. Information is generally either disposed of or sent to the National Archives and Records Administration (NARA) for permanent retention upon expiration of this period. If the system has an applicable SORN(s), check the “Policies and Practices for Retention and Disposal of Records” section.

#### **Section 5.2(a)**

- The records used in the system are covered by a NARA's General Records Schedule (GRS). The GRS is: *General Records Schedule 2.6, Item 030*

### **Section 5.3: E-Government Act/NIST Compliance**

The completion of Federal Information Security Management Act (FISMA) Security Assessment & Authorization (SA&A) process is required before a federal information system may receive Authority to Operate (ATO).

#### **Section 5.3(a)**

- The system last completed an SA&A and received an ATO on: 11-09-2021

#### **Section 5.4: Section 508 of the Rehabilitation Act of 1973**

When Federal agencies develop, procure, maintain, or use Electronic and Information Technology (EIT), [Section 508 of the Rehabilitation Act of 1973](#) (as amended in 1998) requires that individuals with disabilities (including federal employees) must have access and use (including privacy policies and directives as well as redress opportunities) that is comparable to that which is available to individuals who do not have disabilities.

##### **Section 5.4(a)**

- The system complies with all [Section 508](#) requirements, thus ensuring that individuals with disabilities (including federal employees) have access and use (including access to privacy and civil liberties policies) that is comparable to that which is available to individuals who do not have disabilities.

Approval Signature

Bureau Privacy and Civil Library Officer

Date signed: 09-24-2024