

Product Security Bad Practices guidance provides an overview of product security practices that are deemed exceptionally risky, particularly for organizations supporting critical infrastructure or national critical functions (NCFs), and it provides recommendations for software manufacturers to voluntarily mitigate these risks. The guidance contained in the document is non-binding, and while CISA encourages organizations to avoid these bad practices, the document imposes no requirement on them to do so.

The draft guidance is scoped to software manufacturers who develop software products and services, including on-premises software, cloud services, and software as a service (SaaS), used in support of critical infrastructure or NCFs.

By choosing to follow the recommendations in the draft guidance, manufacturers will signal to customers that they are taking ownership of customer security outcomes, a key secure by design principle.

CISA strongly encourage all software manufacturers to avoid the product security bad practices included in the Product Security Bad Practices guidance. The Product Security Bad Practices guidance is co-sealed with the Federal Bureau of Investigation.

III. List of Topics for Commenters

CISA seeks comments on the draft Product Security Bad Practices guidance, in the following three categories. Note: the categories are explained in detail in the draft guidance itself, available at <https://www.cisa.gov/resources-tools/resources/product-security-bad-practices>.

1. Product properties, which describe the observable security-related qualities of a software product itself. Listed bad practices are:

a. A new product line is developed using a memory unsafe language or the manufacturer does not publish a memory safety roadmap by January 1, 2026.

b. The product includes user-provided input directly in the raw contents of a SQL database query string.

c. The product includes user-provided input directly in the raw contents of an operating system command string.

d. The product includes default passwords.

e. The product contains, at the time of release, a component with an exploitable vulnerability present on CISA's Known Exploited Vulnerabilities (KEV) Catalog.

f. The product uses open-source software components that have critical known exploitable vulnerabilities.¹

2. Security features, which describe the security functionalities that a product supports. Listed bad practices are:

a. The baseline version of the product does not support multi-factor authentication.

b. The baseline version of the product does not make audit logs available.

3. Organizational processes and policies, which describe actions taken by a software manufacturer to ensure strong transparency in its approach to security. Listed bad practices are:

a. The organization fails to publish Common Vulnerabilities and Exposures (CVEs) with Common Weakness Enumerations (CWEs) in a timely manner (or at all).

b. The organization fails to publish a vulnerability disclosure policy.

CISA also welcomes comments on other areas or approaches currently absent from the guidance.

This notice is issued under the authority of 6 U.S.C. 652 and 659.

Jeffrey E. Greene,

Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2024-23869 Filed 10-15-24; 8:45 am]

BILLING CODE 9111-LF-P

DEPARTMENT OF HOMELAND SECURITY

[Docket Number DHS-2024-0028]

Agency Information Collection Activities: Office of the Immigration Detention Ombudsman (OIDO) Intake Form, DHS Form 405, OMB Control No. 1601-0030

AGENCY: Department of Homeland Security (DHS).

ACTION: 60-Day notice and request for comments.

SUMMARY: The Department of Homeland Security will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until December 16,

¹ A critical vulnerability is one that has an Attack Vector of "network," Privileges Required of "None," does not require user interaction, and has a "high" impact on at least two of the Confidentiality, Integrity, and Availability loss vectors.

2024. This process is conducted in accordance with 5 CFR 1320.1

ADDRESSES: You may submit comments, identified by docket number Docket # DHS-2024-0028, at:

○ Federal eRulemaking Portal: <http://www.regulations.gov>. Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number Docket # DHS-2024-0028. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

SUPPLEMENTARY INFORMATION: The Department of Homeland Security's (DHS) Office of the Immigration Detention Ombudsman (OIDO) is an independent office tasked with resolving individual complaints from or about individuals in immigration detention regarding the potential violation of immigration detention standards or other potential misconduct. OIDO was established by Congress (sec. 106 of the Consolidated Appropriations Act, 2020, Pub. L. 116-93).

DHS Form 405—"Case Intake Form" is intended for use by individuals wishing to submit a complaint to OIDO. Information collected will provide the office with details about the allegations the submitter seeks to have OIDO address. DHS is revising the information collection to refine several questions in Form 405 and to include an additional form, "Privacy Waiver Authorizing Disclosure to a Third Party". Information collected on the "Privacy Waiver Authorizing Disclosure to a Third Party" will allow OIDO to disclose permitted information to a third party, such as the detained individual's relatives and/or representatives.

The information collected on Form 405—"Case Intake Form" allows OIDO to identify: (1) the individual submitting the complaint and their contact information; (2) the detained individual who is the subject of the complaint; (3) the government-owned or contracted facility where the individual is or was detained and for how long; and (4) relevant details about the complaint. All of this information will be used by OIDO to investigate, resolve, and if appropriate, provide redress.

Based on usability testing recommendations, DHS is revising Form 405. The form will be shortened by reducing extraneous sections, such as Question 12a (Category), Question 12b

(Sub-Category), and Question 16. Please see the Narrative of Changes Table, a supplementary document, noting the revisions.

OIDO will use the additional form, "Privacy Waiver Authorizing Disclosure to a Third Party", to obtain the detained individual's authorization to disclose permitted information and/or records about that individual to a third party. Information collected on the "Privacy Waiver Authorizing Disclosure to a Third Party" will allow OIDO to disclose permitted information to a third party, such as the detained individual's relatives and/or representatives.

The use of DHS Form 405—"Case Intake Form" is the most efficient means for collecting and processing the required data. The form is available for download from the OIDO website. The PDF form can be completed online and submitted to OIDO by email or mail. Additionally, DHS Form 405—"Case Intake Form" can be submitted electronically via the myOIDO portal (<https://myoido.dhs.gov/en-US/>).

After approval of the "Privacy Waiver Authorizing Disclosure to a Third-Party" form, an electronic version will be developed so that submitters may complete and file it via the OIDO website. Additionally, the form will be available for download from the OIDO website. The PDF form will be able to be completed online, printed out, and submitted to OIDO by email or mail or handed in person at a detention facility.

This information collection does not have an impact on small businesses or other small entities. If this information is not collected, OIDO will not be able to accomplish its Congressional mandate to provide assistance to individuals who may be affected by misconduct, excessive force, or other violations of law or detention standards. DHS will conduct this collection in a manner consistent with the general information collection guidelines in 5 CFR 1320.5(d)(2). The assurance of confidentiality provided to the respondents for this information collection is based on the Privacy Impact Assessment for the Immigration Detention Ombudsman Case Management System (IDCMS) (June 21, 2021). Additionally, the information collected is covered by DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361 and DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, June 14, 2017, 82 FR 27274.

This information collection was constructed in compliance with regulations and authorities under the purview of the DHS Privacy Office, DHS OCIO, DHS Records Management, and OMB regulations regarding data collection, use, sharing, storage, information security, and retrieval of information.

The addition of the "Privacy Waiver Authorizing Disclosure to a Third Party" form and the removal of several questions from OIDO "Case Intake Form" resulted in a change in the collection burden.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

Analysis

Agency: Department of Homeland Security (DHS).

Title: Office of the Immigration and Detention Ombudsman (OIDO) Intake Form.

OMB Number: 1601-0030.

Frequency: Annually.

Affected Public: Individuals in Immigration Detention.

Number of Respondents: 5,436.

Estimated Time per Respondent: 1 hour.

Total Burden Hours: 5,436.

Robert Porter Dorr,

Executive Director, Business Management Directorate.

[FR Doc. 2024-23858 Filed 10-15-24; 8:45 am]

BILLING CODE 9112-FL-P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

[FWS-R8-ES-2024-N041;
FXES11130800000-245-FF08E00000]

Endangered and Threatened Wildlife and Plants; Initiation of 5-Year Status Reviews for 59 Pacific Southwest Species

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of initiation of reviews; request for information.

SUMMARY: We, the U.S. Fish and Wildlife Service, are initiating 5-year status reviews under the Endangered Species Act for 59 species. A 5-year status review is based on the best scientific and commercial data available at the time of the review; therefore, we are requesting submission of any new information on these species that has become available since the last reviews.

DATES: To ensure consideration of your information in our reviews, we must receive your comments or information on or before December 16, 2024. However, we will continue to accept new information about any species at any time.

ADDRESSES: For instructions on how to submit information for a species, see table 1 in the **SUPPLEMENTARY INFORMATION** section.

FOR FURTHER INFORMATION CONTACT: To request information on specific species, contact the appropriate person in the table in the **SUPPLEMENTARY INFORMATION** section or, for general information, contact Bjorn Erickson, via phone at (916) 414-6741, via email at peter_erickson@fws.gov, or via U.S. mail at U.S. Fish and Wildlife Service, 2800 Cottage Way, Suite W-2606, Sacramento, CA 95825. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

SUPPLEMENTARY INFORMATION: We, the U.S. Fish and Wildlife Service, are initiating 5-year status reviews under the Endangered Species Act of 1973, as amended (ESA; 16 U.S.C. 1531 *et seq.*), for 32 animal species and 27 plant species. A 5-year status review is based on the best scientific and commercial data available at the time of the review; therefore, we are requesting submission