EVALUATION REPORT

Evaluation of NIST's Management of the National Vulnerability Database

REPORT NO. OIG-26-020-I

MAY 26, 2026

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Office of Audit and Evaluation
Washington, DC 20230

May 26, 2026

MEMORANDUM FOR: Craig Burkhardt
Acting Under Secretary for Standards and Technology and
Acting Director
National Institute of Standards and Technology

FROM: Arthur L. Scott Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *Evaluation of NIST's Management of the National Vulnerability Database*
Report No. OIG-26-020-I

Attached is the final report on our evaluation of the National Institute of Standards and Technology's ability to process vulnerabilities submitted to the National Vulnerability Database in a timely and effective manner. We will post the report on our website per the Inspector General Act of 1978, as amended (5 U.S.C. §§ 404, 420).

Within 60 calendar days, please provide an action plan addressing the report's recommendations, as required by Department Administrative Order 213-5.

We appreciate your staff's cooperation and professionalism during this evaluation.

Attachment

Evaluation of NIST's Management of the National Vulnerability Database

Evaluation Report OIG-26-020-I
May 26, 2026

➤ **What We Audited |** Our objective was to evaluate the effectiveness and sustainability of the National Institute of Standards and Technology's (NIST's) processes for managing cybersecurity vulnerabilities submitted to the National Vulnerability Database (NVD), including the long-term effectiveness of NIST's strategy for reducing its vulnerability backlog and its measures to prevent future processing delays.

➤ **Why This Matters |** The NVD provides crucial data to cybersecurity professionals in the public and private sectors. Through a process called enrichment, NVD analysts update vulnerability records with actionable information that cybersecurity professionals use to prioritize and remediate the vulnerabilities in software and systems. Timely NVD enrichment is essential to defend against cyber threats. A backlog of unprocessed vulnerabilities began in February 2024 and has continued to grow, undermining the NVD's utility and public trust.

➤ **What We Found |** NIST considers the NVD a key piece of the U.S. cybersecurity infrastructure, but its actions to resolve the growing backlog do not reflect that characterization. Specifically, we found:

- NIST's lack of strategic planning and decisive action have allowed the backlog of unprocessed vulnerabilities to continue growing.
- NIST must improve the efficiency of enrichment processes to ensure sustainability. We estimate that NIST could put approximately $800,000 to better use over the next 2 years.
- NIST and the Cybersecurity and Infrastructure Security Agency are operating two vulnerability enrichment programs with significant overlap, which has led to duplicated efforts and wasted approximately $200,000 since May 2024.
- NIST's insufficient communication has frustrated stakeholders and decreased confidence in the NVD.

➤ **What We Recommend |** We made six recommendations to help NIST manage and establish priorities for the NVD, improve the efficiency and sustainability of enrichment processes, and ensure the best use of government resources. NIST concurred with our recommendations and is working to implement them.

Contents

Introduction

Vulnerability management is an essential part of cybersecurity. Identifying and resolving security flaws and weaknesses in IT infrastructure helps prevent cyberattacks, data breaches, and system disruptions. The vulnerability management ecosystem includes government agencies, contractors, and the private sector.

Cybersecurity professionals rely on the National Vulnerability Database (NVD) to identify and act on a range of software and hardware vulnerabilities. The NVD was founded in 2005, and its predecessor dates to 1999. The National Institute of Standards and Technology (NIST), through its Information Technology Laboratory (ITL), is responsible for maintaining the NVD. The bureau considers the NVD to be a key part of the nation's cybersecurity infrastructure.

> Cybersecurity professionals rely on the NVD and the enriched vulnerability data it delivers to discover, prioritize, and remediate vulnerabilities in their software and systems.

Security researchers and vendors submit vulnerabilities identified in software and hardware through the Common Vulnerabilities and Exposures (CVE) Program,[1] which is sponsored by the Cybersecurity and Infrastructure Security Agency (CISA) and is the primary source for NVD content. Each CVE record has a unique identifier[2] and contains structured data about a specific vulnerability. This gives the cybersecurity community a common reference when discussing and addressing it.

Although the NVD relies on the CVE Program, the NVD is a distinct database. Through an automated process, the NVD ingests records from the CVE List[3] within approximately an hour of publication. NVD analysts then enhance CVE records with additional information and analysis (such as severity scores and affected product versions), a process called enrichment. Once enrichment is complete, users and specialized security tools can access the enriched CVE records through the NVD's webpage[4] or automated data feeds. Vulnerabilities that are awaiting or undergoing analysis are considered part of the NVD's backlog of unenriched or unprocessed vulnerabilities.

Prompt enrichment is essential to ensure that the cybersecurity community has the information it needs to discover, prioritize, and remediate vulnerabilities in their software and systems. The NVD analysts who perform enrichment are contractors. Prior to 2024,

[1] The CVE Program is maintained by The MITRE Corporation on behalf of CISA (see https://www.cve.org).

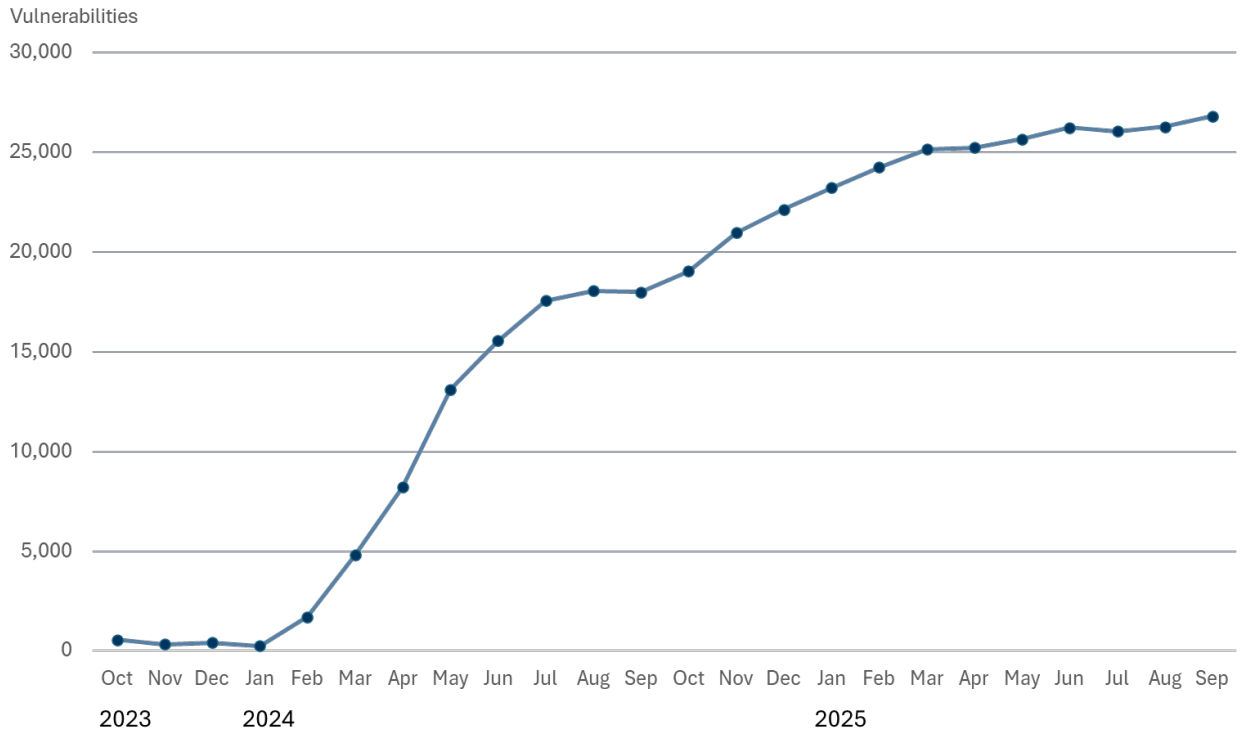
[2] The format for a CVE identifier is standardized, for example CVE-2017-0144.

[3] Available at https://www.cve.org/Downloads.

[4] Located at https://nvd.nist.gov.

NVD analysts were generally able to keep up with processing new vulnerabilities, and the NVD delivered timely, enriched vulnerability data to the public. However, in February 2024, the NVD's enrichment contract lapsed, which contributed to a substantial backlog of unprocessed vulnerabilities that has persisted, as shown in figure 1.

Figure 1. The NVD Backlog Increased Rapidly Starting in February 2024



Source: OIG analysis of NVD data

This backlog has significantly affected both the federal government and the private sector, which rely on timely NVD enrichment to automate vulnerability management and defend against cyber threats. In the 30 days leading up to April 7, 2026, NIST reported that the NVD had approximately 300,000 unique users who downloaded an average of 22 terabytes of data every day.[5] In the absence of real-time enrichment, users are forced to analyze vulnerabilities themselves or turn to other sources (such as commercial products). This raises the likelihood that critical vulnerabilities will be unmitigated and increases the resources required by cybersecurity practitioners to assess risk, triage threats, and prioritize remediation.

[5] NIST provided these numbers as part of its technical comments on our draft report.

Objective

Our objective was to evaluate the effectiveness and sustainability of NIST's processes for managing NVD submission volumes, including the long-term effectiveness of its backlog reduction strategies and measures to prevent future processing delays. Appendix 1 details our scope and methodology.

Findings and Recommendations

Summary: We found that NIST does not have sustainable processes to manage NVD submissions and will be unable to clear the backlog of unprocessed vulnerabilities or prevent future processing delays without significant changes. Specifically, we identified the following issues:

- NIST's lack of strategic planning and decisive action have allowed the backlog of unprocessed vulnerabilities to continue growing.
- NIST must improve the efficiency of enrichment processes to ensure sustainability. We estimate that NIST could put approximately $800,000 to better use over the next 2 years by minimizing its calculation of severity scores.
- NIST and CISA are operating two vulnerability enrichment programs with significant overlap, which has led to duplicated efforts and wasted approximately $200,000 since May 2024.
- NIST's insufficient communication has frustrated stakeholders and decreased confidence in the NVD.

NIST considers the NVD a key piece of the U.S. cybersecurity infrastructure, but its actions to resolve and prevent processing backlogs do not reflect that characterization. Until the backlog is resolved and processes are made sustainable, the NVD will not achieve its mission, and public trust in the NVD will continue to erode.

NIST's Lack of Strategic Planning and Decisive Action Have Allowed the Backlog of Unprocessed Vulnerabilities to Continue Growing

In February 2024, NIST's NVD program experienced a contract lapse that led to a virtual stoppage of vulnerability processing, resulting in an unprecedented backlog. Appendix 2 further details the events leading to this lapse. In May 2024, NIST awarded a new NVD enrichment support contract and publicly communicated that the backlog would be cleared by the end of September 2024. However, internally, NIST did not have a plan or take decisive action to achieve this goal. As a result, the backlog grew from about 13,000 vulnerabilities at the start of June 2024 to over 27,000 by the end of 2025.

We project that in 2026 the yearly total of reported vulnerabilities will surpass 60,000. This represents a nearly tenfold increase from a decade ago, further challenging NIST's ability to resolve the backlog.

Although NIST is authorized to operate the NVD, there are no specific requirements regarding how the NVD should be governed or the results it should produce. This leaves NIST solely responsible for structuring the NVD program to meet stakeholder needs and adapting to changing conditions. Given the public's interest in the program and that NIST considers it a key part of the nation's cybersecurity infrastructure, we requested the NVD strategic plan. According to the Office of Management and Budget's program management standards, strategic planning helps agencies define long-term objectives, necessary actions, and how to respond to challenges.[6]

NIST management informed us, however, that they did not have a strategic plan for the NVD.[7] The lack of a strategic plan likely contributed to NIST's slow and inadequate response to the challenge posed by the backlog. That response included an unrealistic goal, a lack of prioritization given to the processing of critical vulnerabilities, and a delay in the use of alternative resources.

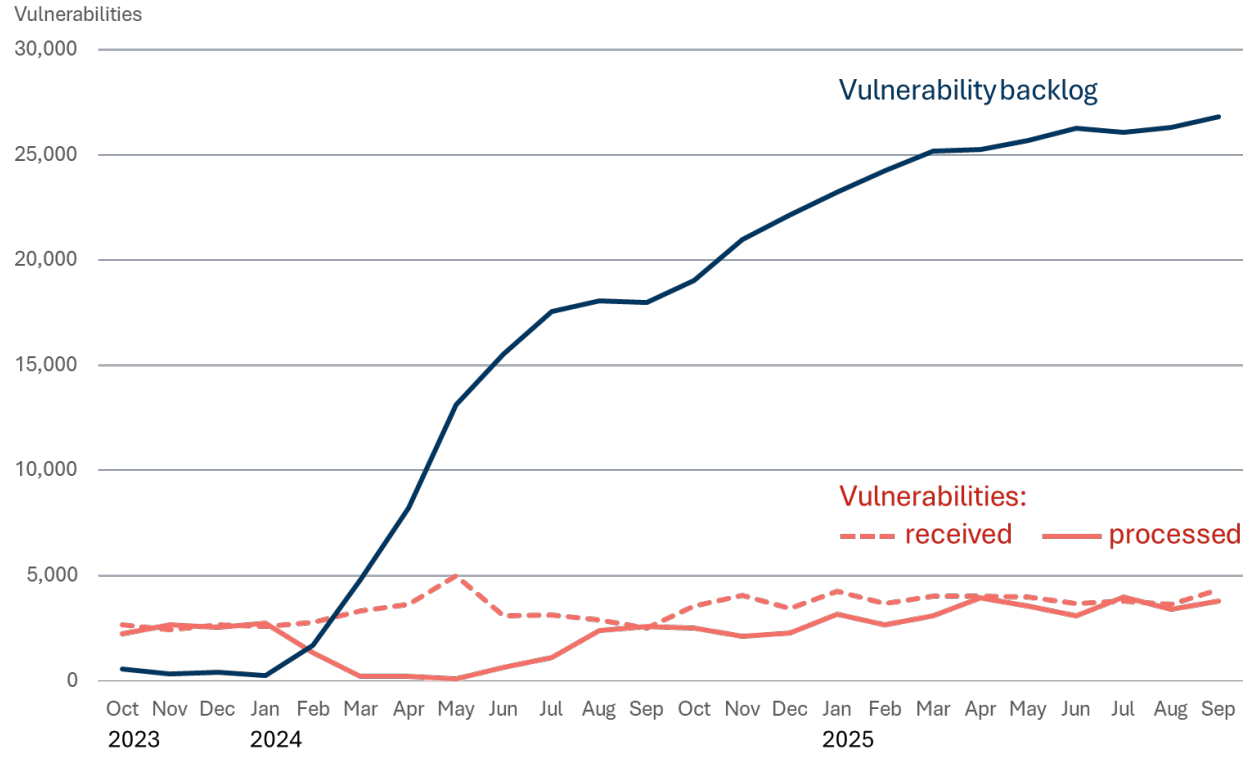
NIST's Goal for Clearing the Backlog Was Unrealistic

At the start of June 2024, the NVD's backlog stood at around 13,000 vulnerabilities. To meet its goal of clearing the backlog by the end of September 2024, NIST needed to process significantly more vulnerabilities than it received. We calculated that NIST needed to process approximately 6,200 vulnerabilities per month—an amount far above its historical capability. In fact, NIST failed to process more vulnerabilities than it received during that timeframe and has not processed more than 5,000 vulnerabilities in any month. Thus, the backlog continued to grow, as shown in figure 2.

[6] Office of Management and Budget. August 29, 2025. "What government-wide standards and principles for program and project management have been developed and how should they be applied?" (section 270.2), *Preparation, Submission, and Execution of the Budget,* circular A-11.

[7] After we asked about a strategic plan, management told us they had begun developing one, but it was not finished in time for our review.

Figure 2. The Number of Vulnerabilities Processed Was Insufficient to Address the Backlog



Source: OIG analysis of NVD data

NIST reported that, after the contract lapse in February 2024, the NVD did not have a fully trained team of analysts until November 2024. As a result, its capacity to perform enrichment was reduced during that timeframe. Further, NVD enrichment was just one task within a larger support contract. NIST assigned contracted analysts to work on other programs or complete non-enrichment tasks,[8] which also reduced the total number of hours available for enrichment. Still, we estimated that even if all analysts had been fully trained and assigned to NVD enrichment, NIST could have processed around 5,300 vulnerabilities per month—below the 6,200 it needed to meet the September goal.

NIST increased its target processing rate in May 2025, reducing the total expected enrichment time for each vulnerability. However, by the end of 2025, the backlog continued to grow and had more than doubled from its starting June 2024 total. Even so, management assigned non-enrichment tasks to analysts and had not set a new target date to resolve the backlog.

[8] Analysts were assigned to spend time on other tasks such as responding to stakeholder emails or supporting NIST's National Checklist Program.

NIST Did Not Effectively Prioritize the Processing of Critical Vulnerabilities

NIST officials told us that as the backlog grew they followed a process to prioritize (i.e., complete before others) the enrichment of the most critical vulnerabilities. These included vulnerabilities receiving considerable public attention, those affecting widely used products, and those in CISA's Known Exploited Vulnerabilities (KEV) Catalog.[9] Because vulnerabilities in the KEV Catalog are actively used by attackers, CISA recommends that organizations immediately prioritize them for remediation. Furthermore, federal civilian executive branch agencies are required to remediate vulnerabilities in the KEV Catalog within 2 weeks. Thus, the faster NVD analysts complete enrichment for these vulnerabilities, the sooner critical information is available to help users with remediation.

Although NIST's process identified which vulnerabilities to prioritize, it did not specify what constituted *timely* enrichment for NVD analysts, which, as described above, is a key requirement of KEV remediation. Considering their criticality, we determined that 1 weekday was a reasonable timeframe for NVD analysts to identify and enrich vulnerabilities that are added to the KEV Catalog. Our testing found that enrichment from February 2024 to December 2025 was not timely for 34 percent of KEV Catalog vulnerabilities.[10]

NIST Was Slow to Use Alternative Enrichment Sources

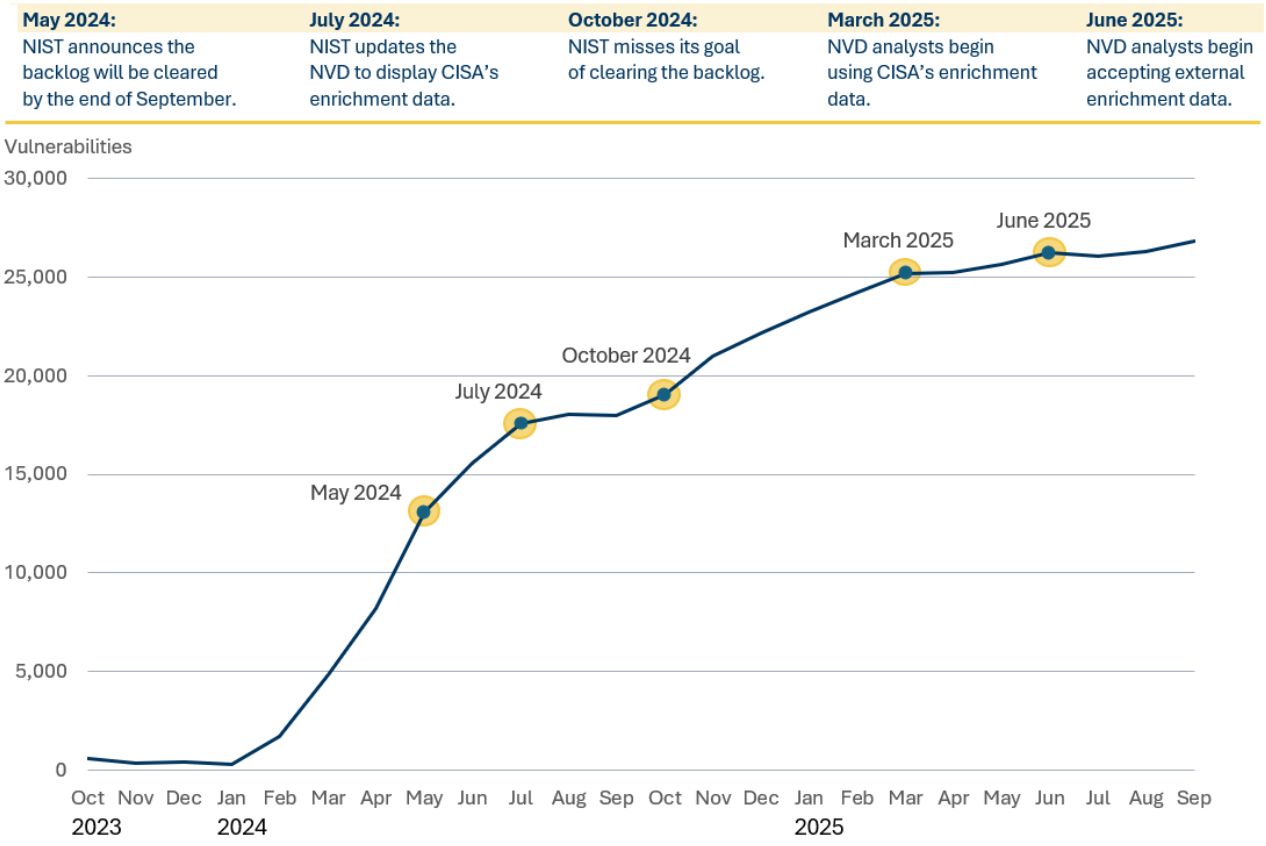
In May 2024, CISA began providing its own enrichment data for vulnerabilities separate from the NVD. As discussed later in the report, CISA completes nearly all of the same enrichment activities as NIST; therefore, an opportunity existed for NIST to leverage CISA's data to expedite backlog reduction. However, NIST officials stated that the NVD system required technical updates to incorporate CISA's enrichment data because the system lacked the capability to attribute data to specific sources.

Due to the way NIST's internal enrichment system worked, NVD analysts were required to complete all fields before publishing a record. Before the final system update and subsequent process change in March 2025, NIST was unwilling to use CISA's data because it would have appeared as if an NVD analyst had performed the enrichment. While it is understandable that NIST wanted to be clear about the source of data in the NVD, it ultimately delayed vulnerability processing to distinguish whether enrichment was completed by NIST or CISA—both federal agencies with access to the same public information. Figure 3 highlights NIST's slow response alongside the growing backlog.

[9] CISA maintains this catalog as the authoritative source of vulnerabilities that have been exploited.

[10] For our analysis, we reviewed a total of 226 KEVs that (1) had been identified as KEVs between February 2024 and December 2025 and (2) had not already been analyzed by NIST at the time of identification.

Figure 3. NIST Was Slow to Take Action as the Backlog Grew



Source: OIG analysis of NVD data

To make informed decisions and take decisive action, officials needed to fully understand the NVD's role in the overall vulnerability management ecosystem and the needs of its stakeholders. Absent a strategic plan or equivalent document, NIST officials had insufficient guidance on how to balance the NVD's traditionally independent enrichment against resolving the mounting backlog. With submission volumes growing, NIST will be increasingly challenged to keep pace and meet future demands, potentially worsening the backlog. Without a strategy, even if NIST were to instantly clear the backlog today, a new backlog would soon begin to form.

Recommendations

We recommend that the Under Secretary of Commerce for Standards and Technology instruct the ITL Director to:

1. Create a strategic plan for the NVD that reflects the NVD's role in the overall vulnerability management ecosystem, establishes priorities, and ensures long-term sustainability of processing capacity.
2. Establish a backlog management plan that includes (1) an analysis of constraints and capacity, (2) a target date for resolving the backlog, (3) milestones to meet that goal, and (4) processes that prioritize critical vulnerabilities.

NIST Must Improve the Efficiency of Enrichment Processes to Ensure Sustainability

In addition to NIST's actions to address the NVD backlog, we also evaluated two of the four activities NVD analysts complete as part of the enrichment process for each vulnerability.[11] These two key activities, severity scoring and assigning product applicability statements, consumed an estimated 80 percent of the enrichment processing time. Improving the efficiency of these core activities is NIST's best opportunity to create a sustainable enrichment process.

NIST's Calculation of Severity Scores May No Longer Be Necessary

To generate a severity score for vulnerabilities, NIST uses the industry standard Common Vulnerability Scoring System (CVSS).[12] Although the standard is well defined, our review found that implementation is highly dependent on available information and professional judgment. In our internal testing, severity scores were consistent among independent OIG evaluators just 12 percent of the time.[13] We concluded that severity scores vary depending on who performs the work and the information available to them. In a technical comment on our draft report, NIST stated that "NVD analysts receive several months of training and all scores are double-checked to ensure normalization." Still, NVD analysts only have access to publicly released information to generate scores, while those provided directly by a software vendor may be based on nonpublic information.

[11] Table 1 in the next finding describes each of the four enrichment activities.

[12] For ease of reading, we refer to CVSS scores as "severity scores" throughout the report.

[13] See appendix 1 for a description of our methodology.

As of August 2025, nearly 80 percent of CVE Program participants included severity scores in vulnerability submissions, and CISA provided severity scores for submissions without them as part of its own enrichment program. Traditionally, NIST calculated its own independent severity score for each vulnerability. NIST stated that it did so as part of its mandate to determine the nature and extent of information security vulnerabilities[14] and independently assign severity metrics to identified vulnerabilities.[15] However, NIST is not required to calculate a severity score for every vulnerability. Today, this approach may no longer be necessary and, considering the increasing volume of vulnerability submissions, is no longer sustainable.

In fact, NIST adopted a "gap-filling" approach to address the increasing backlog in June 2025. Under this approach, NIST would no longer score a vulnerability if another party had already provided a severity score. However, this change was not formalized in policy, and NIST reported that it continued to check whether external scores were reasonable. As of December 2025, we found instances where NIST was still providing its own scores for vulnerabilities that had been scored by another party, thus duplicating efforts. NIST officials noted that vulnerability submitters may provide biased scores and NVD analysts provide value through independent verification. However, NIST did not provide evidence of biased scoring. Therefore, our testing concluded that if a score already exists, analysts' time would be better spent on other parts of the enrichment process. Were NIST to minimize its calculation of severity scores, we estimate that it could put approximately $800,000 to better use over the next 2 years.[16]

Assigning Applicability Statements Is Manual and Time Consuming

Analysts spend the majority of the NVD enrichment process assigning a Common Platform Enumeration (CPE)[17] applicability statement to each vulnerability. These statements define affected product versions and configurations using a standardized, machine-readable format (that a computer can process automatically). NIST is solely responsible for maintaining the CPE dictionary of the standardized names used to build applicability statements, which are critical for automated vulnerability management.

---

[14] According to 15 U.S.C. § 278g-3(d)(3)(A), NIST must "conduct research and analysis to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security[.]"

[15] According to 42 U.S.C. § 18933(a), NIST must "assign severity metrics to identified vulnerabilities with open source software."

[16] See appendix 1 for a description of our methodology and appendix 3 for a summary of potential monetary impacts.

[17] CPE is a structured naming scheme for information technology systems, software, and packages.

Creating a CPE applicability statement is a manual and time-consuming process, especially when the relevant products are not already listed in the dictionary. Although some software vendors attempt to provide the CPE applicability statement when submitting vulnerabilities, even large organizations have struggled to format statements according to NIST's standards. This results in NVD analysts having to re-create the submitted entries. Additionally, NIST does not currently offer a tool for external parties to update or submit content to the CPE dictionary. Instead, updates are submitted via email, and NVD analysts must manually process each request. The time NVD analysts spend on this task is time taken away from clearing the backlog or processing new vulnerabilities.

In recognition of these challenges, NIST has made improvements to internal tools that help NVD analysts complete CPE applicability statements more efficiently. NIST is also developing a console to allow external contributions to the CPE dictionary, which could increase efficiency by reducing the amount of time spent compiling lists of software or hardware versions. Instead, vendors will be able to supply CPE dictionary entries in a format NIST accepts.

NIST must improve the efficiency of creating CPE applicability statements, which are the most time-consuming activity of its enrichment process. In fact, CISA stopped creating applicability statements in December 2024, in part due to how long it took to prepare them. NIST is now the sole government source for this crucial data, making it even more critical that the process be sustainable.

Recommendations

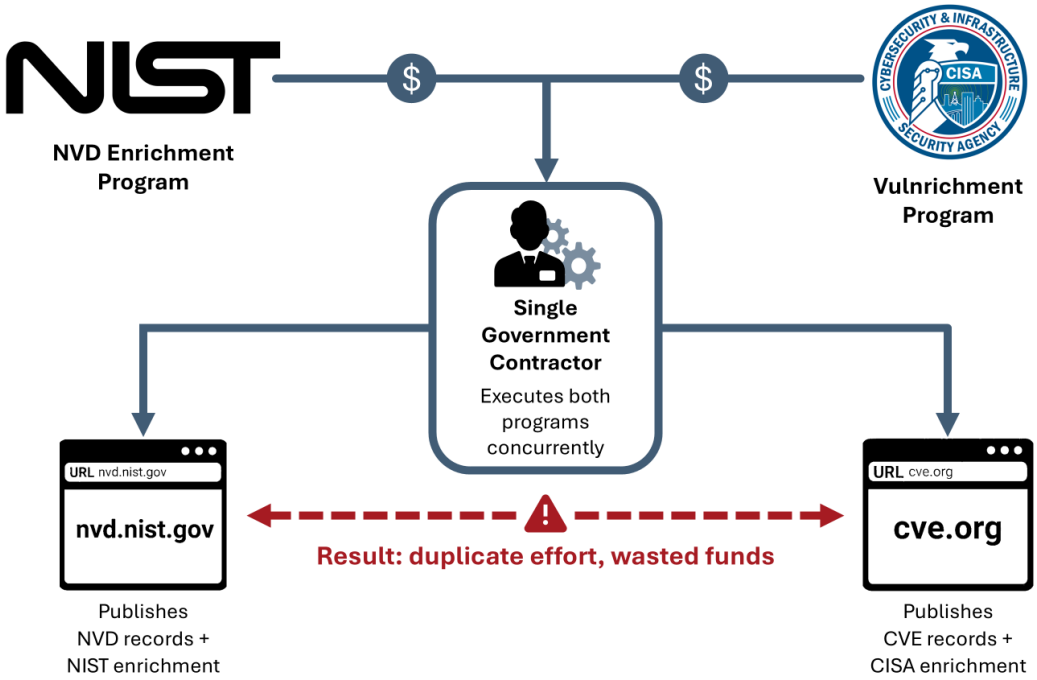
We recommend that the Under Secretary of Commerce for Standards and Technology instruct the ITL Director to:

3. Define in policy a strategy to minimize NIST's efforts to calculate severity scores. Implementing this recommendation can put approximately $800,000 to better use.
4. Ensure that the NVD has an efficient method for external parties to contribute to the enrichment of CPE applicability statements.

NIST and CISA Are Operating Two Vulnerability Enrichment Programs with Significant Overlap, Leading to Duplicated Efforts and Wasted Funds

For over 20 years, the NVD has been a key source for vulnerability data. In May 2024, as NIST dealt with the lapsed enrichment contract and the resulting backlog, CISA launched its own vulnerability enrichment program, called Vulnrichment. At the time, CISA invited NIST to collaborate and issue a joint statement about the new program. However, NIST did not take part in a joint statement or issue any announcement about CISA's program. Ultimately, the two programs have operated without coordination and have duplicated enrichment activities, as shown in figure 4.

Figure 4. Overlap of Federal Vulnerability Enrichment Programs



Source: OIG analysis of enrichment programs

Enrichment includes several activities. Both the NVD and Vulnrichment programs categorize the type of vulnerability, assign a severity score, and provide reference information. When Vulnrichment launched, it also identified the products affected by a vulnerability through CPE applicability statements. As discussed previously, CISA stopped creating CPE applicability statements in December 2024, leaving the NVD as the only federal provider of this service.[18] Vulnrichment also completes an additional activity,

[18] CISA noted that its analysts spent most of their enrichment time on identifying affected products.

stakeholder specific vulnerability categorization (SSVC), which is a vulnerability prioritization methodology intended to guide organizations during their remediation efforts.[19] Table 1 captures the overlap between the two programs' enrichment activities.

Table 1. Comparison of NIST and CISA Enrichment Activities

Enrichment Activity	NIST NVD	CISA Vulnrichment
Assign a severity score using the CVSS	✓	✓
Categorize the cause using CWE	✓	✓
Define affected products (names and versions) via a CPE applicability statement	✓	✗*
Determine the significance using SSVC	✗	✓
Identify relevant references using publicly available sources	✓	✓

Source: OIG analysis of enrichment programs

Abbreviations: CPE = Common Platform Enumeration, CVSS = Common Vulnerability Scoring System, CWE = Common Weakness Enumeration, SSVC = Stakeholder-Specific Vulnerability Categorization

* CISA generated CPE applicability statements from May to December 2024.

At the time of our fieldwork, CISA had been operating Vulnrichment for over a year. The program was clearly not a temporary response to the NVD's issues, and the government was now operating and paying for two overlapping vulnerability enrichment programs. Still, NIST and CISA did not coordinate their enrichment processes. Further, both programs used the same contractor and, in some cases, performed the same enrichment activities.[20] We identified at least 21,000 instances from May 2024 through December 2025 when NIST and CISA duplicated enrichment activities.[21]

The lack of coordination between programs led directly to duplicative work. NVD analysts attempted to avoid enrichment activities that had already been completed by CISA, but CISA analysts sometimes completed and published their work on vulnerabilities that were

[19] See CISA, "Stakeholder-Specific Vulnerability Categorization (SSVC)," accessed March 16, 2026.

[20] Regarding severity scores, NIST noted that it is statutorily mandated to assign severity metrics to identified vulnerabilities with open source software. However, the law does not specifically mandate the use of CVSS nor does it require calculating a score.

[21] We considered an enrichment activity to be duplicated if both CISA and NIST completed the same activity for a vulnerability. For example, if both agencies calculated a vulnerability severity score, we considered it to be a duplicate activity regardless of whether the scores differed. We then used NIST's estimates and our own observations to determine the average time spent on each duplicated activity and calculate wasted funds.

still undergoing analysis in the NVD. This meant that an NVD analyst had effectively duplicated the enrichment activities that were also completed by CISA.

Using NIST's contract rates, we estimate that NIST spent approximately $200,000 on duplicate enrichment activities since the launch of the Vulnrichment program in May 2024.[22] Our estimate represents only the funds spent directly on enrichment activities and does not capture funds spent on program overhead. By coordinating their enrichment efforts, NIST and CISA may uncover further opportunities to reduce spending. Without such coordination, the government will continue to waste money on overlapping enrichment programs.

Recommendation

We recommend that the Under Secretary of Commerce for Standards and Technology instruct the ITL Director to:

5. Immediately begin coordinating with CISA to avoid duplicate enrichment activities and ensure the best use of government resources. Implementing this recommendation will prevent duplicate efforts that have already led to $200,000 in waste.

NIST's Insufficient Communication Has Frustrated Stakeholders and Decreased Confidence in the NVD

On April 12, 2024, over 50 cybersecurity professionals with vulnerability management expertise sent an open letter to Congress and the Secretary of Commerce urging them to investigate "the lack of transparent communication from NIST regarding regression in NVD operations."[23] The organizer of the open letter said that neither NIST nor the Department of Commerce provided a response.

We surveyed the parties who signed the open letter and found that they remained frustrated with NIST's lack of transparency. Ninety percent of respondents were dissatisfied with the frequency of NIST's updates on the state of the backlog, and 75 percent reported relying less on the NVD for vulnerability management since the backlog began. However, 80 percent of respondents agreed that the NVD provides unique

[22] See appendix 3 for a summary of potential monetary impacts.

[23] Lorenc, Dan, Nic Chaillan, Omkhar Arasaratnam, et al. *An Open Letter from Cybersecurity Professionals to the U.S. Congress and Secretary of Commerce*. April 12, 2024.

enrichment data, which shows that the NVD does offer a valuable service—but that it also needs to engage and inform its stakeholders.

In April 2024, the ITL Director asked the NIST public affairs office for support with NVD external communications. Yet we continued to see examples of poor communication to NVD stakeholders. From at least March 2025 to July 2025, the NVD did not present accurate data on its online dashboard for two fields showing critical information on the status of vulnerabilities.[24] An inaccurate dashboard made it difficult for NVD stakeholders to fully understand how many vulnerabilities were in the backlog. Further, as described in our first finding, NIST missed its goal of clearing the backlog by the end of September 2024. We reviewed the NVD's official communications web page[25] and found that NIST had not announced a new goal. In fact, as of the end of 2025, the last update regarding the backlog was over 9 months old.

The Foundations for Evidence-Based Policymaking Act of 2018 required the Government Accountability Office (GAO) to identify best practices to ensure that federal programs are achieving their intended results. GAO found that stakeholder engagement is vital to the success of federal efforts and should happen early and often rather than as a one-time event.[26] Key stakeholders for the NVD are the users who rely on the database to make informed decisions regarding vulnerability management.

Traditionally, the NVD has been the authoritative source for freely accessible vulnerability information, supporting NIST's claim that the NVD is a key piece of the nation's cybersecurity infrastructure. However, NIST's poor communication regarding the NVD's status has left stakeholders with less confidence that the NVD will be readily available to provide timely and accurate vulnerability enrichment. In December 2025, NIST officials told us that they were developing a strategic plan for the NVD and planned to engage with key stakeholders as part of its development. Establishing a communication strategy as part of the strategic plan could help restore stakeholders' confidence in the NVD.

➤➤ NIST's poor communication has left stakeholders less confident that the NVD can provide timely and accurate vulnerability enrichment. ➤➤

[24] The two fields on the NVD dashboard were "Undergoing Analysis" (how many vulnerabilities are going through the enrichment process) and "Received" (how many vulnerabilities have been added to the NVD).

[25] The NVD's official communication page is located at https://www.nist.gov/itl/nvd.

[26] GAO. July 2023. *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts,* GAO-23-105460, 43.

Recommendation

We recommend that the Under Secretary of Commerce for Standards and Technology instruct the ITL Director to:

6. Develop a communication strategy to keep stakeholders informed and instill confidence in the NVD.

Conclusion

NIST's management of the NVD has not been sufficient to resolve the backlog or to keep pace with the growing volume of vulnerability submissions. Despite recognizing the NVD as critical cybersecurity infrastructure, NIST has not adopted a strategy to ensure that the NVD has a sustainable future. Unsustainable enrichment processes, lack of coordination with CISA, and poor communication with stakeholders have undermined the NVD's utility and public trust. Without significant changes to how it is managed, the NVD will not be a reliable piece of the nation's cybersecurity infrastructure.

Summary of NIST's Response and OIG's Comments

NIST reviewed a draft version of this report and responded to our findings and recommendations. In its response, NIST concurred with all of our recommendations and described actions it has taken or plans to take to address them. NIST's complete response, which also included general comments, is included in this report as appendix 4. We address comments from NIST's response below.

NIST also provided technical comments on the draft report. We considered these comments and revised the report where appropriate. NIST's full technical comments are included in appendix 5.

We are pleased that NIST concurs with our recommendations. We look forward to receiving NIST's action plan, which will provide details on its corrective actions.

OIG's Comments on NIST's Response

Feedback from NIST regarding the draft report largely described a broader statutory and historical narrative as context for NVD operations and suggested that our evaluation was incomplete. Our evaluation objective, however, centered on management effectiveness and program sustainability during a defined period. Within that scope, the report's findings are supported by documented facts on backlog causation, capacity, timeliness, duplication, and communication.

In this final report, where appropriate for context and understanding, we have added language about statutory authorities for the NVD. However, as noted in the report, there are no specific statutory requirements for precisely how the NVD should be governed or the results it should produce. We have considered the statutes identified by NIST, and we re-affirm our statement that the cited authorities generally do not provide methods for how NIST must operate the NVD, nor do they explicitly reference the NVD. Our recommendations are congruent with NIST's own management actions[27] and are designed to improve outcomes without impeding statutory responsibilities.

[27] Following receipt of our draft report, NIST publicly announced updates to NVD operations, on April 15, 2026, that aligned with our recommendations. For example, we recommended that NIST minimize its efforts to conduct severity scoring. As part of its update, NIST announced that it will only enrich vulnerabilities that meet its new criteria, meaning it will no longer assign a score for each vulnerability.

Finally, we disagree with NIST's assertion that the report did not follow the Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) *Quality Standards for Inspection and Evaluation*. As stated in appendix 1, our evaluation complied with CIGIE's latest standards and requirements. Furthermore, we maintain an internal quality control system that has been scrutinized through periodic peer reviews, the results of which are published in our *Semiannual Report to Congress*.

Appendix 1. Scope and Methodology

Our evaluation objective was to evaluate the effectiveness and sustainability of NIST's processes for managing NVD submission volumes, including the long-term effectiveness of its backlog reduction strategies and measures to prevent future processing delays. Our scope was NIST's management of the NVD from October 2023 to December 2025. We used interviews, walkthroughs, document analysis, and questionnaires to determine how the NVD backlog occurred and whether NIST had effective plans to both resolve the backlog and prevent a future one.

To assess how the backlog occurred and whether NIST had effective plans to resolve it and prevent a future one, we:

- Reviewed the following documents:
    - NVD program contracts
    - NVD vulnerability enrichment policies and procedures
    - NVD team meeting notes and analysis reports
    - CISA-NIST interagency agreement and statement of work
- Attended a walkthrough with NVD analysts at NIST's Gaithersburg, Maryland, campus to understand NIST's enrichment process for the NVD
- Interviewed NVD program leadership, NVD analysts, industry stakeholders, and NVD partners, such as CISA
- Issued a questionnaire to cybersecurity leaders to understand their perception of NIST's communications
- Learned about the federal government's support for the CVE Program infrastructure, including MITRE's CVE.org, CISA's Vulnrichment, and NIST's NVD

To test the consistency of CVSS or severity scores, we randomly sampled 72 vulnerabilities. The sample was then divided among three OIG cybersecurity specialists for scoring, with each vulnerability being analyzed twice. Using the CVSS 3.1 specifications, cybersecurity specialists created CVSS vector strings, which serve as the basis of a CVSS score. Of the 72 selected vulnerabilities, 69 were successfully analyzed. Of the 69 vulnerabilities, cybersecurity specialists produced the same vector string just 8 times (12 percent). We also expanded our testing to use an AI model and found a similar level of inconsistency.

We relied on computer-processed data to support our findings, conclusions, and recommendations. Specifically, we used NIST's NVD data feeds and application

programming interface to gather our data. OIG data analysts assessed the data and found it to be sufficiently reliable to support our findings and conclusions.

We conducted our evaluation from June 2025 through April 2026 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424), and Department Organization Order 10-13, as amended October 21, 2020.

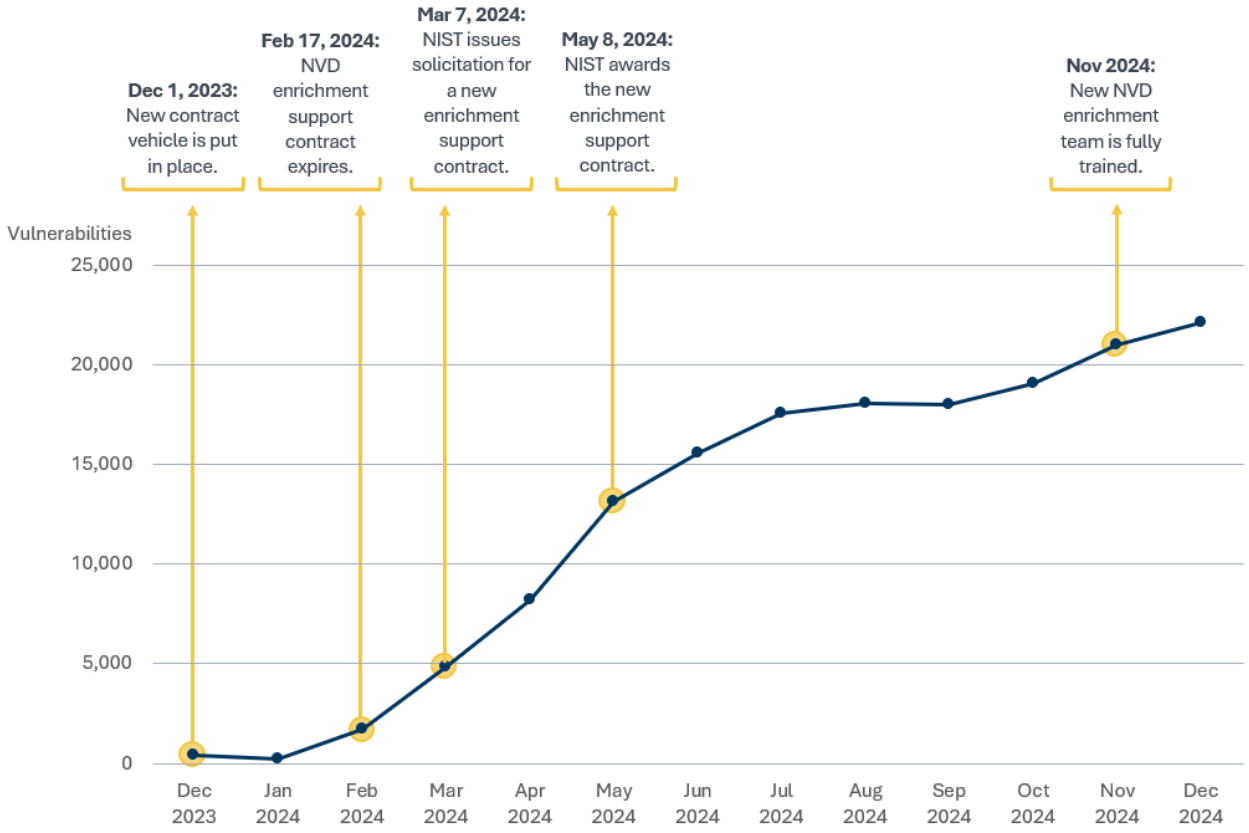
We conducted this evaluation in accordance with *Quality Standards for Inspection and Evaluation* (December 2020) issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that the evidence must sufficiently and appropriately support evaluation findings and provide a reasonable basis for conclusions and recommendations related to the objective. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our review objective.

Appendix 2. Formation of the NVD Backlog

The NVD's historic backlog stemmed from two challenges: transitioning the NVD enrichment support contract and maintaining NVD funding.

NIST relies almost exclusively on a single contractor to support NVD enrichment activities, via a delivery order under a larger contract vehicle.[28] As early as July 2022, NIST management knew that their current contractor would not be eligible to participate in renewal of the enrichment support contract.[29] To avoid interruptions in vulnerability processing, NIST needed to transition to a new contractor prior to February 2024. However, a new contract was not put in place until May 2024, and the new team of NVD analysts was not fully trained until November 2024. Figure 5 notes key events related to the contract transition.

Figure 5. Renewal of the NVD Enrichment Support Contract Was Delayed While the Vulnerability Backlog Grew



Source: OIG analysis of NIST data

[28] NIST uses an indefinite delivery-indefinite quantity contract as a vehicle to solicit and award enrichment support delivery orders.

[29] The authority NIST used to issue the enrichment support contract required the awardee to be a small business. In January 2021, NIST's original contractor was acquired by a larger company that was not eligible.

Notably, NIST also faced a significant funding challenge as it moved through the contract renewal process. In recent years, CISA had provided financial support for the NVD through an annual interagency agreement with NIST.[30] In FY 2023, CISA provided nearly $3.8 million—approximately half of the NVD's total funding for that year. However, CISA did not renew its financial support for the NVD in FY 2024.

Despite its new financial position, the division chief overseeing the NVD was unwilling to request additional funds and cited other competing priorities at ITL. It was not until over a month after NVD enrichment effectively stopped in February 2024 that NIST leadership transferred additional funds to support a new enrichment contract.

[30] NIST and CISA entered into interagency agreements using the transfer authority of the NIST Organic Act, 15 U.S.C. §§ 273, 275a, and 278b.

Appendix 3. Potential Monetary Impacts

Table 2 summarizes the questioned costs we identified. We categorize questioned costs as either (1) unallowable or unreasonable or (2) unsupported.

1. An unallowable or unreasonable cost is a cost that we determined does not comply with governing law, regulation, contract, or agreement or that should not have been charged to the government because it is not justifiable or necessary.
2. An unsupported cost is a cost that we determined is not supported by adequate documentation.

Table 2. Summary of $200,000 in Questioned Costs

Finding	Recommendation	Unallowable or Unreasonable Costs	Unsupported Costs
NIST and CISA Are Operating Two Vulnerability Enrichment Programs with Significant Overlap, Leading to Duplicated Efforts and Wasted Funds	5	$200,000	–
Totals	–	**$200,000**	–

Source: OIG analysis of NVD data

Table 3 summarizes funds we identified that NIST could put to better use. A recommendation to put funds to better use is based on our conclusion that the funds could be used more efficiently—for example, via reducing spending or deobligating funds.

Table 3. Summary of $800,000 to Be Put to Better Use

Finding	Recommendation	Funds to Be Put to Better Use
NIST Must Improve the Efficiency of Enrichment Processes to Ensure Sustainability	3	$800,000
Total	–	**$800,000**

Source: OIG analysis of NVD data

Appendix 4. NIST's Response

NIST's response to our draft report begins on the next page.

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

OFFICE OF THE DIRECTOR

April 23, 2026

MEMORANDUM FOR Arthur L. Scott, Jr.
Assistant Inspector General for Audit and Evaluation

From: Craig S. Burkhardt, J.D.
Acting Under Secretary of Commerce for Standards and Technology &
Acting Director, National Institute of Standards and Technology

Subject: National Institute of Standards and Technology's Response to the Office of the Inspector General's Draft Report dated April 2, 2026, *Evaluation of NIST's Management of the National Vulnerability Database*

Thank you for the opportunity to respond to the OIG draft report entitled *Evaluation of NIST's Management of the National Vulnerability Database.*

The Department agrees with the recommendations and will prepare a formal action plan upon issuance of OIG's final report. However, as detailed in the attached comments submitted by the NIST Office of Chief Counsel, the Department notes that the draft report does not sufficiently address certain statutory requirements that impact NIST's management of the NVD, nor does the report satisfy the high standards set forth in the Council of Inspector General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (QSIE), which require reports present information in a fair and objective manner; that reports be complete and accurate; and that reports provide readers with the legal and factual context necessary for a complete understanding of the operation of the program or activity.

Finding 1: NIST's lack of strategic planning and decisive action have allowed the backlog of unprocessed vulnerabilities to continue growing.

- **OIG's Recommendation #1:** Create a strategic plan for the NVD that reflects the NVD's role in the overall vulnerability management ecosystem, establishes priorities, and ensures long-term sustainability of processing capacity.

  Agency Response: NIST concurs with this recommendation. NIST's Information Technology Laboratory (ITL) is developing an initial draft strategic plan and will further develop and finalize it based on feedback from stakeholder engagements.

- **OIG Recommendation #2**: Establish a backlog management plan that includes (1) an analysis of constraints and capacity, (2) a target date for resolving the backlog, (3) milestones to meet that goal, and (4) processes that prioritize critical vulnerabilities.

  Agency Response: NIST concurs with this recommendation. NIST is drafting a backlog management plan and will further develop and finalize it based on feedback from stakeholder engagements. NIST is also preparing a new process for prioritizing critical vulnerabilities.

Finding 2: NIST must improve the efficiency of enrichment processes to ensure sustainability. Were NIST to fully stop severity scoring, OIG estimates that it could put approximately $800,000 to better use over the next 2 years.

- **OIG's Recommendation #3:** Define in policy a strategy to minimize NIST's efforts to calculate severity scores. Implementing this recommendation can put approximately $800,000 to better use.

  Agency Response: NIST will no longer routinely calculate severity scores for CVEs that already have them. In the event a severity score is clearly not consistent with the CVSS specification or the publicly available information, NIST may still provide a severity score. NIST will also provide a severity score as resources allow if a request is made for NIST to provide one. NIST is also exploring automated mechanisms to conduct severity scoring.

- **OIG Recommendation #4**: Ensure that the NVD has an efficient method for external parties to contribute to the enrichment of CPE applicability statements.

  Agency Response: NIST concurs with this recommendation. NIST is evaluating options to provide this capability and to potentially broaden product applicability statements beyond CPE names.

Finding 3: NIST and CISA are operating two vulnerability enrichment programs with significant overlap, which has led to duplicated efforts and wasted approximately $200,000 since May 2024.

- **OIG's Recommendation #5:** Immediately begin coordinating with CISA to avoid duplicate enrichment activities and ensure the best use of government resources. Implementing this recommendation will prevent duplicate efforts that have already led to $200,000 in waste.

  Agency Response: NIST concurs with this recommendation. NIST's ITL has contacted CISA and will coordinate to ensure CVE enrichment processes are complementary and not duplicative.

Finding 4: NIST's insufficient communication has frustrated stakeholders and decreased confidence in the NVD.

- **OIG's Recommendation #6:** Develop a communication strategy to keep stakeholders informed and instill confidence in the NVD.

  Agency Response: NIST concurs with this recommendation. NIST's ITL and Communications and Outreach Office are working together to develop a communication strategy.

If you have any questions, please contact Amy Egan, Audit Liaison, at (307) 975-2819 or amy.egan@nist.gov.

National Institute of Standards and Technology Office of Chief Counsel Comments on the OIG Draft Report entitled: *Evaluation of NIST's Management of the National Vulnerability Database*

The National Institute of Standards and Technology Office of Chief Counsel (NIST OCC) has reviewed the Office of the Inspector General (OIG) Draft Report dated April 2, 2026 (Draft Report) in conjunction with the Department of Commerce (Department) and offers the following comments. In short, while NIST OCC concurs with the recommendations set forth in the Draft Report, NIST OCC does not concur with the Draft Report because it fails to fully and accurately account for NIST statutory obligations and contains characterizations that are likely to mislead readers.

The Draft Report is expected to satisfy the high standards set forth in the Council of Inspector General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (QSIE). Indeed, on page 17, the Draft Report certifies that it does so, asserting that the underlying evaluation was "conducted . . . in accordance" with the QSIE and that the "findings, conclusions, and recommendations" contained in the Draft Report are consistent with the standards set forth in the QSIE. For the reasons set forth below, NIST OCC believes that the Draft Report does not meet those standards.

I. The Draft Report Does Not Present Information in a Fair and Objective Manner.

Under Standard 5 of the QSIE, OIG inspections reports must "present factual data accurately, fairly, and objectively, and present findings, conclusions, and recommendations in a persuasive manner." The Draft Report falls short of this requirement at numerous points. For example, on page 3, the Draft Report contains the following statement: "NIST considers the [National Vulnerability Database (NVD)] a key piece of the U.S. cybersecurity infrastructure, but its actions to resolve and prevent processing backlogs do not reflect that characterization." Rather than assess the impact of NIST's actions in a fair, factual, and objective manner, this statement unnecessarily casts doubt on NIST's intentions and priorities. The Draft Report is replete with language that goes beyond objective, factual evaluation.

II. The Report Is Incomplete.

Under section 5.1b of the QSIE, reports should be "complete" and "accurate." The Draft Report, however, fails to account for—let alone even discuss—several of the statutory authorities and obligations related to NVD. For example:

a. Nowhere in the Draft Report is there any mention of NIST's statutory obligations to operate and carry out specific functions as part of the NVD.

i. Under 15 U.S.C. § 272 (b)(5) and (c)(12), (14), (15), (18), and (27) of NIST's organic statute, NIST is required to establish a "clearinghouse[1] of current information" and "on an ongoing basis, facilitate and support" standards, methodologies, and processes to reduce cyber risks, and compile, evaluate, and publish technical data resulting from such performance of these functions. The Federal Information Modernization Act of 2014[2] ("FISMA")[3] and the American Innovation and Competitiveness Act, further broadened NIST's authorities and obligations to operate the NVD under 15 U.S.C. §278g-3(d)(3)(A), directing NIST to submit standards to be enforced by the Department of Homeland Security and the Office of Management and [as part of FISMA]; and to provide assistance to agencies regarding detecting and handling information security incidents, and conduct research and analysis to determine the extent of information security vulnerabilities, and to carry out research associated with improving the security and integrity of the information technology supply chain. While it might be argued that the statutes referenced above do not expressly call for the National Vulnerability Database, the term "clearinghouse," combined with NIST's Organic Act obligations and FISMA strongly support the necessary creation of the NVD to comply with such requirements. *See Footnotes 1 and 2.* Further, support can be derived from the legislative history of the NVD program.[4]

---

[1] The NVD is a database established, in part, as a means to satisfy this statutory obligation. Notably, in the U.S. Code, the term "clearinghouse" is used in a number of statutes to describe centralized systems for collecting, organizing, and disseminating information. In practice, these provisions have often led federal agencies to stand up databases, portals, or data-sharing platforms that function as modern "clearinghouses." Examples include: the ERIC Clearinghouse System (20 U.S.C. § 1221e-3) at the Department of Education; the National Criminal Justice Reference Service (NCJRS) at the Justice Department (34 U.S.C. § 10141); the National Health Information Clearinghouses at the U.S. Department of Health and Human Services (42 U.S.C. § 242k); and the Environmental Information Clearinghouses at the Environmental Protection Agency (42 U.S.C. § 4375), among others.

[2] Although no single statute explicitly mandates the NVD, NIST's obligations can be derived from FISMA and related authorities. Specifically: (1) Data standardization and publication: NIST must provide standardized vulnerability data to support federal cybersecurity programs. This includes: Aggregating CVE entries; Assigning severity metrics (e.g., CVSS scores); and Maintaining machine-readable formats for automation; (2) Support for Federal Risk Management: Under FISMA, agencies must implement risk-based security programs. NIST supports this by: Providing authoritative vulnerability data; Enabling continuous monitoring frameworks; and Supporting compliance validation tools; and (3) Public Accessibility and National Infrastructure Role: The NVD is publicly accessible and supports both federal and private-sector cybersecurity efforts, reflecting NIST's broader statutory mission to promote U.S. economic and technological security.

[3] The Federal Information Security Modernization Act of 2014 amended the Federal Information Security Management Act of 2002. *See* 44 U.S.C. §§ 3551–3558. Under FISMA, agencies are required to adopt and comply with standards promulgated by NIST related to information security for federal information systems (44 U.S.C. § 3553). These standards include risk management, vulnerability identification, and continuous monitoring frameworks. The NVD is expressly recognized as part of NIST's implementation of these responsibilities: it serves as the "U.S. government repository of standards-based vulnerability management data" supporting FISMA compliance and automation. Thus, while the NVD itself is not separately codified, it is a core operational mechanism through which NIST fulfills FISMA-mandated responsibilities.

[4] The enactment of FISMA in 2002 significantly expanded NIST's cybersecurity responsibilities, including: formalizing NIST's role in developing federal security standards; driving demand for centralized vulnerability data;

b. Further, nowhere in the Draft Report is it acknowledged that NIST is required to provide severity scores for open-source software vulnerabilities under 42 U.S.C. § 18933(a); and under 15 U.S.C. § 287g-3c(b)(1), to disseminate that information and have such information be aligned with industry best practices and Standards set forth under the International Organization for Standardization (ISO); nor does it contemplate these authorities (referenced below) would potentially drive NIST to include the Common Platform Enumeration (CPE) applicability statements.
    i. The IoT Improvement Act (15 U.S.C. § 278g–3c) which authorizes, among other things, NIST to develop guidelines related to vulnerability disclosure.
    ii. The Draft Report also fails to mention under E.O. 14028 – Improving the Nation's Cybersecurity (2021), Section 4(e)(viii) which also directs NIST to issue guidance identifying practices that enhance the security of the software supply chain, including procedures regarding "participating in a vulnerability disclosure program that includes a reporting and disclosure process."

c. Additionally, nowhere in the OIG Draft Report does it mention that the NVD is a federal dataset managed by NIST, and as such is required to follow the Foundations for Evidence-Based Policymaking Act of 2018 governing how agencies manage, share, and use data as a strategic asset.
    i. The NVD complies with the Act's open data requirements by providing publicly accessible, machine-readable vulnerability data through APIs and structured feeds, consistent with 44 U.S.C. § 3506(b)(6) and § 3506(d)(2). It maintains detailed schemas, metadata, and documentation describing its datasets, aligning with federal requirements for comprehensive data inventories and metadata under 44 U.S.C. § 3511(a)(1)–(2). The NVD also adheres to standardized data formats such as CVE, CVSS, and CPE, supporting interoperability and data standards as directed by 44 U.S.C. § 3504(d)(1). Finally, by enabling risk analysis, cybersecurity research, and policy evaluation across agencies, the NVD supports evidence-building activities consistent with agency learning agendas and evaluation functions under 5 U.S.C. § 312(a)–(b).

Had the OIG inspection considered these necessary criteria, the report would not have included statements that have the potential to mislead readers by inaccurately omitting the NVD's legal obligations. Examples include:

---

and establishing the need for automated compliance tools (leading to ISAP and the NVD). Thus, FISMA is the primary legislative driver behind the NVD's development and expansion. Subsequent legislative and policy developments—while not always directly referencing the NVD—further expanded its role. Later statutes, including the Cybersecurity Information Sharing Act of 2015 and the Cybersecurity and Infrastructure Security Agency Act of 2018, reinforced the federal government's emphasis on information sharing and vulnerability management ecosystems, indirectly strengthening the importance of the NVD.

i. "Were NIST to fully stop severity scoring, we estimate that it could put approximately $800,000 to better use over the next 2 years." (p. 3)

    a. By law, NIST is required to assign severity scoring.

ii. "Both the NVD and Vulnrichment programs categorize the type of vulnerability, assign a severity score, and provide reference information. When Vulnrichment launched, it also identified the products affected by a vulnerability through CPE applicability statements. As discussed previously, CISA stopped creating CPE applicability statements in December 2024, leaving the NVD as the only federal provider of this service. Vulnrichment also completes an additional activity, stakeholder specific vulnerability categorization (SSVC), which is a vulnerability prioritization methodology intended to guide organizations during their remediation efforts." (p. 11)

    a. This characterization and comparison suggest to the reader that the NVD and the Vulnrichment program are substantially similar programs which may lead readers to conclude that NIST's work is duplicative and inefficient. In particular, the report notes that CPE statements are manual and time-consuming, but the report omits the fact that NIST is required to incorporate CPE statements.[5] The report also fails to mention in any depth the use and necessity of CPE statements for software supply chain security. It also further fails to discuss the Foundations for Evidence-Based in Policymaking Act ("Evidence Act"). The NVD is the gold standard for compliance and structure in having its datasets fully meet the Evidence Act governance, transparency, and standardization requirements. CISA's Vulnrichment is directionally aligned with the Evidence Act and already performs well as an operational, open dataset. However, compared to a mature benchmark like NVD, Vulnrichment would need more formalization, documentation, and transparency to fully meet the Act's expectations around data governance, metadata, and evidence-building rigor.

III. The Report Fails to Provide Readers with the Legal Context Necessary for a Complete Understanding.

[5] NIST is required under 15 U.S.C. § 278g–3c and E.O. 14028 to develop guidelines for vulnerability disclosure. These guidelines require CPE statements, and as such, CPE statements must be included to comply with best practices.

The QSIE sets forth several requirements pertaining to a how inspectors must develop their findings, conclusions, and recommendations, which include collecting evidence to support the analysis necessary for making recommendations, and including limitations of the inspection. Specifically, section 5.2 of the QSIE provides that "[i]nspectors must base report findings, conclusions, and recommendations on the evidence collected and the analysis conducted during the inspection," that under 5.2b "[i]nspection reports should describe any limitations so that readers have context for the findings, conclusions, and recommendations."

Based on the methodology and scope of the report discussed in Appendix 1, and the overall report, the OIG Draft Report fails in its criteria (per 3.3a and 3.4 of the QSIE) to consider laws and regulations applicable to the operation of the program or activity, or performance of similar entities.

a. Had the OIG also considered discussing the limitations of the scope of this report (per Appendix 1 and the requirements under the QSE handbook to discuss limitations) the report might also have noted that the OIG would not comment on- nor assess the efficacy or legal obligations of CISA's vulnerability database and program, and it might have considered that CISA's vulnerability program is not subject to the same requirements of the Evidence Act, the Federal Information Security Modernization Act, sections of the Chips & Science Act, and other cybersecurity laws charging NIST with specific authorities. **Examples of where this might have provided context include:**

    i. "NIST and CISA are operating two vulnerability enrichment programs with significant overlap, which has led to duplicated efforts and wasted approximately $200,000 since May 2024." (p. 6)

        1. NIST OCC points out that CISA initiated a program duplicating NIST's statutory mandate.

    ii. "To generate a severity score for vulnerabilities, NIST uses the industry standard Common Vulnerability Scoring System (CVSS). Although the standard is well defined, our review found that implementation is highly dependent on available information and professional judgment." (p. 8)

        2. NIST OCC notes that reliance on CVSS is itself a standards-based requirement.

    iii. "Were NIST to fully stop severity scoring, we estimate that it could put approximately $800,000 to better use over the next 2 years." (P. 9)

3. NVD is required to engage in severity scoring.

iv. "NIST must improve the efficiency of creating CPE applicability statements, which are the most time-consuming activity of its enrichment process. In fact, CISA stopped creating applicability statements in December 2024, in part due to how long it took to prepare them." (p. 10)

4. This comparison is inapt because NIST has a statutory obligation. Without this context, the statement may lead readers to view the NVD as less efficient, when in fact NIST is fulfilling mandatory statutory responsibilities. NVD in practice (based on its mandate to support standards development and adhere to such standards for FISMA purposes where developing federal cybersecurity risk management frameworks) is required to carry out the CPE statements until alternative standards and frameworks are developed and adopted to carry out NIST's software vulnerability supply chain mission.

IV. The Report Does Not Provide Readers with the Factual Context Necessary for a Complete Understanding.

As noted above, the QSIE sets forth several requirements pertaining to how inspectors must develop their findings, conclusions, and recommendations. Section 5.3a of the QSIE provides that "[i]nspection reporting should give the reader the context in which the subject matter being inspected should be viewed. The report should enable the reader to understand the impact or significance of the operation, program, policy, or entity being inspected and the relevance of the findings, conclusions, and any recommendations."

The OIG draft also fails to provide the reader with necessary context to understand the NVD program and separately the timing of the backlog aligning with a surge of CVEs generated with the rise of AI.

a. By comparing the operation of NIST's NVD program and mission to that of CISA's mission and operation of Vulnrichment, without discussing any statutory history or background of the two programs, their authorities or mandates, the reader is left without an understanding of the relationship of the two agencies and programs to one another or their evolution, which would shed light on the agencies' cybersecurity roles and interdependence, and on the history of CISA providing support to NIST in funding the NVD database.

Even if the OIG were to suggest that the inclusion of such history could possibly be deemed outside of the scope of this report, such an assertion would appear to cut against the content in the Introduction section of the report (p.1). The report's introduction includes *some* history on the NVD and its relationship to CISA. Yet, that background contains omissions of other historical and legal facts, that would likely lead the reader to have significantly different impressions and conclusions about the operation and function of NIST and CISA's cybersecurity programs that such reader likely would not have if given more information. For example:

The NVD and NIST's role in tracking cyber vulnerabilities significantly predates the Department of Homeland Security's cyber programs. The NVD's precursor (the ICAT) was initially launched in the late 1990s as part of early federal vulnerability tracking initiatives. In the early 2000s, the enactment of FISMA in 2002[6] significantly expanded NIST's role in federal cybersecurity by mandating the development of standards and guidelines. This statutory framework created the need for centralized, standardized vulnerability data to support agency compliance, risk management, and automated security assessment. As a result, the NVD was formally established in 2005 to meet these needs and support FISMA implementation.[7] Later statutes, including the Cybersecurity Information Sharing Act of 2015 and the Cybersecurity and Infrastructure Security Agency Act of 2018, reinforced the federal government's emphasis on information sharing and vulnerability management ecosystems, indirectly strengthening the importance of the NVD. Meanwhile, the Department of Homeland Security derived its cybersecurity authorities from laws passed after the 2002 FISMA, under the Homeland Security Act of 2002 (6 U.S.C. § 101 et seq.); and subsequent amendments, including the National Cybersecurity and Critical Infrastructure Protection Act of 2014, and the Cybersecurity and Infrastructure Security Agency Act of 2018.

Whereas NIST derives a substantial amount of its cybersecurity authority from FISMA, DHS and CISA, by contrast, derive their authority from the Homeland Security Act and related statutes to conduct operational cybersecurity activities, including vulnerability response and enforcement.

The legislative history and framework demonstrate that Congress has intentionally and consistently chosen to establish a framework where NIST and DHS (CISA) take on different, complimentary cybersecurity responsibilities in coordination with one another. For example, FISMA (2014) established a clear division of responsibilities

[6] Pub. L. No. 107-347, Title III

[7] See NIST, *NVD Overview*; NIST SP 800-126 Rev. 3 (describing the role of NVD in SCAP and FISMA compliance)

between the two agencies by directing NIST to develop standards and guidelines. The intersection between NIST and DHS/CISA responsibilities can be summarized as follows: NVD provides standardized vulnerability data; CISA prioritizes, responds to, and mandates remediation of vulnerabilities; and NIST standards inform CISA directives and federal agency compliance obligations. NIST Special Publication 800-216 (2023) highlights the importance of coordinated vulnerability disclosure programs and references statutory authorities for federal vulnerability handling, including DHS authorities under 6 U.S.C. § 659(m). This structure reflects Congress's intent to separate technical standard-setting from operational cybersecurity execution.

The OIG draft additionally failed to provide full context for funding challenges related to the NVD program.

a. While the report did correctly note that CISA provided NIST nearly $3.8 million in FY 2023 (approximately half of NVD yearly funding) and no funding to NIST in FY 2024, the report did not note that the NIST budget for laboratory programs was also reduced by approximately $20 million from FY 2023 to FY 2024. During this time, the Division running NVD requested additional resources, noting NVD lacked sufficient resources. On multiple occasions, one-time NIST-level funding was granted, providing partial support for the NVD program, though the amounts were not enough to cover the full funding deficit. The one-time funding came in the form of reprioritized NIST-level carryover funding ($2.285M in FY24) and ITL lab director discretionary funding ($2.0M in FY25). The IG was aware of these requests and the provision of funding. And yet, instead of providing the context of specific significant loss of funds to the NVD program specifically and to NIST laboratory programs at large, the OIG draft instead characterized these funding issues for the NVD program as a lack of willingness to request additional funds.

Other examples of where context would have supported the reader's understanding of the program in accordance with the QSIE include:

b. Had the relevant laws or limitations of the inspection of the above elements been included as criteria as part of the report's conclusions, recommendations, and findings, it is ostensibly less likely that OIG would be able to support its findings in Appendix 3, discussing Monetary Impacts.

   If the OIG criteria had taken into account NIST's NVD obligations and authorities, or the limitations of commenting on CISA's obligations and statutory role in relation to NIST's NVD under FISMA, then the OIG might have determined while funds were not efficiently used, saying they could be put to better use for other

purposes is not entirely accurate. Given that NVD informs the standards and risk management framework underpinning the nation's cybersecurity law for critical infrastructure (FISMA). It is unclear what better use of funds there might be than to empower NVD to lead the public and private sector in vulnerability standards, scoring and application.

c. Additionally, had context been provided as to when the NVD enrichment contract lapsed and its coinciding with the widespread use of artificial intelligence and the rapid proliferation of discovered vulnerabilities, the reader would have been more fairly informed of the findings and conclusions.

   The charts provided on page 5 of the report and page 18 in the Appendix 2 show a surge in the NVD backlog. Interviews with NVD staff would highlight that CVE submissions have increased 263 percent between 2020 and 2025.

Appendix 5. NIST's Technical Comments

NIST's technical comments on our draft report begin on the next page.

National Institute of Standards and Technology Comments
on the OIG Draft Report entitled *Evaluation of NIST's Management of the National Vulnerability Database*

The National Institute of Standards and Technology (NIST) has reviewed the draft report and our comments are below. Page numbers refer to page numbers in the report unless otherwise stated.

General Comments

Please see separate NIST OCC response for additional comments.

NIST notes that the draft report may not sufficiently address certain statutory requirements that impact NIST's management of the NVD.

These requirements include that:

- NIST "shall— conduct research and analysis— to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security." 15 U.S.C. § 278g-3 (d)(3)(A).
- The NIST "Director shall assign severity metrics to identified vulnerabilities with open source software and produce voluntary guidance to assist the entities that maintain open source software repositories to discover and mitigate vulnerabilities." 42 USC § 18933(a).
- The NIST Director "shall develop and publish under section 278g–3 of this title guidelines— for the reporting, coordinating, publishing, and receiving of information about— a security vulnerability relating to information systems owned or controlled by an agency…" and the "guidelines published under subsection (a) shall— to the maximum extent practicable, be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization (or any successor standard) or any other appropriate, relevant, and widely-used standard." 15 U.S.C. § 278g-3c(a)(1)(A) and (b)(1).

Recommended Changes for Factual/Technical Information

Page 2, second paragraph, second sentence:
The statistics provided were accurate at the time they were provided. Please update the sentence to indicate the date or other context for these statistics. For the 30 days leading up to April 7, 2026, there were an average of 301,505 unique visitors per day, and an average of 22 terabytes per day.

Page 3, second bullet under the summary section, second sentence:
This sentence uses the phrase "fully stop" while recommendation 3 says to "minimize" which may be misleading if someone were to only read the summary and not read the individual recommendations.

Page 4, first full paragraph, first sentence:
Although NIST is authorized to operate the NVD, there are only a small number of specific requirements regarding how the NVD should be governed or the results it should produce. Other than these requirements, this leaves NIST solely responsible for structuring the NVD program to meet stakeholder needs and adapting to changing conditions.

Page 8, third paragraph, fourth sentence:
CVSS scores supported by publicly available information permit cybersecurity professionals to make accurate response and mitigation plans. Encouraging vendors and CNAs to provide robust public information to aid responders in developing such plans is to the benefit of the vulnerability ecosystem.

Page 8, fourth paragraph, second sentence:
Traditionally, NIST has calculated its own independent severity score for each vulnerability as NIST felt mandated to independently conduct research and analysis to determine the nature and extent of information security vulnerabilities and independently assign severity metrics to identified vulnerabilities. However, NIST's mandate to assign severity metrics may not require independent, duplicative calculation of severity scores for every identified vulnerability, and this approach may no longer be necessary. Indeed, considering the increasing volume of vulnerability submissions, this approach is no longer sustainable.

Page 10, Table 1:
Assign a severity score using the CVSS†
† NIST is statutorily mandated to assign severity metrics to identified vulnerabilities with open source software.

Page 16, third paragraph:
The result identified in this paragraph is an example of why the NVD provides a score. NVD analysts receive several months of training, and all scores are double-checked to ensure normalization. NVD follows a consistent scoring methodology based on the CVSS specification and publicly available information allowing for as close to an apples-to-apples comparison between vulnerabilities issued by different vendors as possible.

Editorial Comments
No comments.

REPORT

FRAUD & WASTE & ABUSE

HOTLINE

Department of Commerce

Office of Inspector General Hotline

www.oig.doc.gov | 800-424-5197