Congressional Budget Office
Nonpartisan Analysis for the U.S. Congress

ANSWERS TO QUESTIONS FOR THE RECORD

Following a Hearing on

CBO's Appropriation Request for Fiscal Year 2024

Conducted by the
Subcommittee on the Legislative Branch
Committee on Appropriations
United States Senate

APRIL 6 | 2023

On March 15, 2023, the Subcommittee on the Legislative Branch of the Senate Committee on Appropriations convened a hearing at which Phillip L. Swagel, the Congressional Budget Office's Director, testified about the agency's appropriation request for fiscal year 2024.[1] *After the hearing, Chairman Reed and Ranking Member Fischer submitted questions for the record. This document provides CBO's answers. It is available at* www.cbo.gov/publication/59030.

Chairman Reed's Questions About CBO's Cybersecurity Efforts

Question. In CBO's FY 24 budget request, the agency is requesting increases to continue to address cybersecurity requirements. How is CBO keeping up with the expectation and demand for maintaining the highest level of cybersecurity within the agency?

Answer. CBO works with security experts to remain up to date with threats. The agency receives support from a security operation center (SOC) and third-party vendors to ensure compliance with certain National Institutes of Standards and Technology (NIST) guidelines and updates from the Cybersecurity and Infrastructure Security Agency and other information technology (IT) security authorities to maintain the highest level of cybersecurity. CBO's security team regularly completes vulnerability scans. The agency also participates in the legislative branch's ThreatStream solution, which legislative branch agencies use to share threat intelligence information. FireEye and CheckPoint are other tools the agency currently uses to mitigate and reduce threats. Finally, CBO meets with vendors regularly to stay abreast of upgrades in technology that could enhance the agency's security posture.

For the most sensitive information that CBO receives from other federal agencies, it must provide the same level of cybersecurity as those agencies. For that reason, CBO also hardens its systems in accordance with those agencies' requirements. CBO's principles for sensitive but unclassified (SBU) security engineering encompass a variety of precepts regarding the design, development, specifications, implementation, and maintenance of a secure cloud-based virtual desktop infrastructure environment. CBO follows the guidance in NIST 800-160 Volume 1 as part of a continuing effort to improve the security of its IT environment.

During the fiscal planning, budget request, and budget allocation processes, CBO's senior information security engineer works with the agency's chief information officer and the chief administrative officer to review existing system requirements and identify new ones that would aid in the protection of the agency's information technology infrastructure, systems, and data. Those requirements are reflected in a detailed line-item spreadsheet and are reflected as must-fund requirements.

Question. How are you guarding against insider threat?

Answer. CBO's current insider threat program includes annual training for all staff, monitoring for unusual activity through security and IT controls, and log monitoring. The agency's privacy officer, general counsel's office, chief information officer, enterprise architect, and information systems security officer work together to make decisions necessary for the agency's overall risk program, which includes insider threat detection and prevention.

The review process for CBO's analytic work includes steps to guard against disclosure of sensitive information. To protect against accidental disclosure, CBO provides computer-based training to all staff annually; more specific training modules are assigned to staff on the basis of their roles and data access. Insider threat training is included as part of that annual security training.

Staff members are required to undergo background checks before using sensitive data. Those data are processed in distinct enclaves that are segregated from CBO's normal operations. Movement of data within those enclaves is monitored, and any extraction of data from those enclaves follows a peer-review and approval process. Tools to protect against data loss are used to monitor and provide alerts about suspicious outgoing email.

CBO also actively guards against exfiltration—that is, unauthorized transfer of data from its systems. CBO's SOC reviews the system logs that are forwarded to its Security Information Enterprise Management (SIEM)

[1] See testimony of Phillip L. Swagel, Director, Congressional Budget Office, before the Subcommittee on the Legislative Branch of the Senate Committee on Appropriations, *The Congressional Budget Office's Request for Appropriations for Fiscal Year 2024* (March 15, 2023), www.cbo.gov/publication/58985.

solution. Within SIEM, those logs are monitored and triaged if issues are found. SIEM includes a behavior analytics module that is triggered when security anomalies appear. If an incident is identified, the privacy officer is notified pursuant to CBO's incident response plan.

Question. How are you ensuring that technology that is being purchased and used within CBO is free from cyber vulnerability?

Answer. Before purchasing software, CBO reviews products for their suitability, legality, and level of security. As part of that effort, the agency analyzes the potential for risk on the basis of software function, vulnerability vectors, code security reviews, and participation in bug-hunting and issue-reporting programs. The agency's procurement staff reviews vendors for their reputability using a variety of sources, including basic financial and banking information. When applicable, CBO uses technology that has achieved at least a moderate rating from the Federal Risk and Authorization Management Program.

After procurement and before use, all equipment is inspected by the Capitol Police, who take custody of all deliveries for legislative branch agencies. They perform physical inspections for evidence of tampering and dangerous materials. Subject matter experts unpack and inspect new equipment and apply tamper-evident inventory tags that help CBO identify and track equipment during each stage of its life cycle. If the equipment will store or process SBU, an SBU-specific tamper-evident tag is also applied.

Equipment taken by staff for travel is assigned from a specific pool; upon the staff member's return, the equipment is returned to IT for sanitization and reimaging. Annual checks of randomly selected pieces of IT equipment are conducted to confirm asset tags, locations, and serial numbers.

CBO conducts vulnerability scans across its systems each month to ensure that they are secure as part of the agency's vulnerability management process. CBO performs updates in response to threat advisories from our vendors and partners. The agency also has a change management process in place to review and approve system change requests for potential security implications before implementation.

Ranking Member Fischer's Question About CBO's Transparency Efforts

Question. CBO's FY24 budget request notes the importance of enhancing transparency of the agency's analysis. Given the role CBO plays in projecting costs and impacts of legislation, more transparency is a worthy goal. Can you detail some of CBO's recent transparency improvement efforts and how the FY24 request will expand upon them?

Answer. Transparency is a top priority for CBO, and the agency continues to bolster such efforts. Those efforts are intended to promote a thorough understanding of its work, help people gauge how estimates might change if policies or circumstances differed, and enhance the credibility of its analyses and processes.

In 2022, some highlights of CBO's transparency efforts included the following:

- **Releasing data.** *The Budget and Economic Outlook: 2022 to 2032*, *An Analysis of the President's 2023 Budget*, and several other reports were supplemented with comprehensive sets of data files. In total, 43 reports were accompanied by files providing the data underlying their figures.
- **Explaining its analytic methods.** CBO published various reports explaining its analyses and made supporting documents and some computer code available. Also, in many cost estimates, CBO included a section describing the basis for the estimate.
- **Analyzing the accuracy of its estimates.** CBO released a comprehensive report about the accuracy of its budget projections for fiscal year 2021. To do that, CBO focused on its March 2020 baseline projections and updated them to include the estimated effects of subsequently enacted legislation. That analysis indicated that CBO overestimated the federal deficit in 2021—the result of underestimating revenues and overestimating outlays.
- **Estimating the effects of policy alternatives.** CBO prepared reports and created interactive products to estimate the effects that alternative assumptions about future policies would have on economic and budgetary outcomes. In the two volumes of *Options for Reducing the Deficit, 2023 to 2032*, the agency described 76 policy options that would decrease federal spending or increase federal revenues over the

next decade. Other products examined the effects of policies that would change the prices insurers pay for hospitals' and physicians' services, work requirements for recipients of means-tested benefits, the age of eligibility for Medicare, and the minimum wage.

In 2023 and 2024, almost all of CBO's employees will spend part of their time on efforts to make the agency's analyses more transparent. In particular, the fiscal year 2024 budget request will enable CBO to enhance its transparency activities in the following ways:

- Provide additional information to help people understand the federal budget process and CBO's role in that process; and
- Explain the methods it uses for its analyses in several topic areas, including national security, climate change, and economic projections.

Those efforts will build on CBO's current activities, which include testifying before Congressional committees and answering Members' questions, releasing data, evaluating the accuracy of the agency's estimates, comparing current estimates with previous ones, estimating the effects of policy alternatives, characterizing the uncertainty surrounding estimates, creating data visualizations, and conducting outreach.[2]

[2] For a review of CBO's transparency activities in 2022 and a forecast of future work, see Congressional Budget Office, *Transparency at CBO: Future Plans and a Review of 2022* (March 2023), www.cbo.gov/publication/58930. A continually updated list of the agency's most recent activities is available at www.cbo.gov/about/transparency.