CROSS-SECTOR CYBERSECURITY PERFORMANCE GOALS

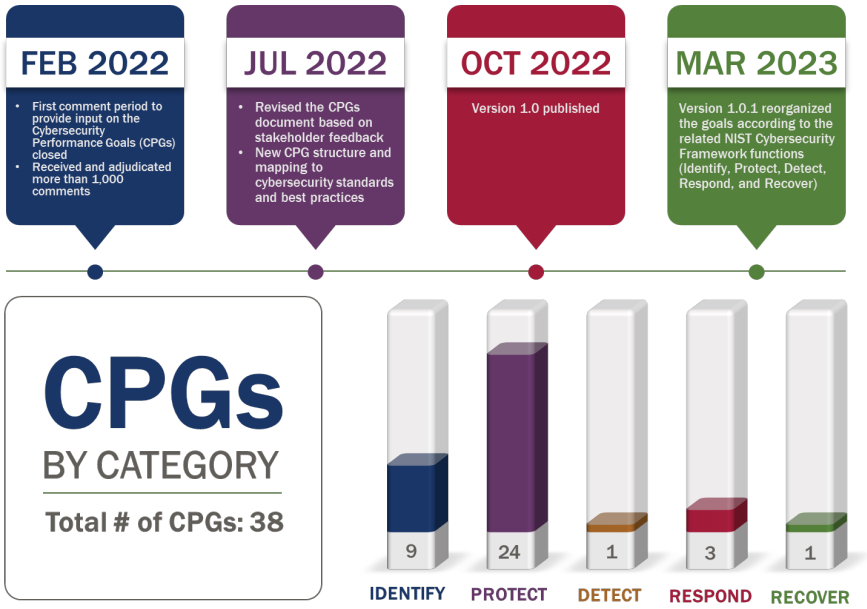
OVERVIEW

Organizations across every sector are under constant threat from malicious cyber actors. At the same time, every organization has limited resources to implement effective cybersecurity measures, leading to a simple question: where to start? The cross-sector Cybersecurity Performance Goals (CPGs) are intended to help answer this question by providing a prioritized subset of information technology (IT) and operational technology (OT) cybersecurity practices aimed at meaningfully reducing risk to both critical infrastructure operations and the American people. The CPGs allow organizations to align investments and assess gaps based upon the most common and impactful threats and adversary tactics, techniques, and procedures (TTPs) observed by the Cybersecurity and Infrastructure Security Agency (CISA) and its government and industry partners, making them a common set of protections that all critical infrastructure entities — from large to small — should implement.

DEVELOPMENT PROCESS

In July 2021, President Biden signed National Security Memorandum (NSM)-5: Improving Cybersecurity for Critical Infrastructure Control Systems. NSM-5 required CISA, in coordination with the National Institute for Standards and Technology (NIST) and the interagency community, to develop baseline CPGs that are consistent across all critical infrastructure sectors.

As part of the CPG development process, CISA gathered feedback from Sector Risk Management Agencies, Sector Coordinating Councils, and other sector partners that collected guidance from key OT/Industrial Control Systems subject-matter experts. By working collaboratively with partners to ensure their input throughout the baseline CPG development process, CISA drove cross-sector buy-in and ensured the development of goals that were more traceable and easier to implement.



NIST CYBERSECURITY FRAMEWORK (CSF) ALIGNMENT

After CISA published the first CPG report in October 2022, the agency received feedback from multiple sectors asking for more streamlined orientation to the NIST Cybersecurity Framework (CSF). In response, CISA reorganized the CPGs to align to the NIST CSF functions (Identify, Protect, Detect, Respond, and Recover) in the March 2023 Version 1.0.1 release. This alignment is intended to help organizations more easily use CPGs to prioritize investments as part of a broader cybersecurity program built around the CSF. The CPGs are a prioritized subset of the NIST CSF categories and subcategories and do not identify all the cybersecurity practices needed to protect every organization or fully safeguard

national and economic security and public health and safety. The CPGs will be reviewed and updated as needed following the release of NIST CSF Version 2.0.

FORMAT AND DELIVERY

The CPG assessment is offered through the Cyber Security Evaluation Tool (CSET®). CSET® is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets, offering more than 60 different cybersecurity assessments. This tool is a downloadable, stand-alone desktop application that provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks.

Within CSET®, the 38-question CPG assessment can be done through self-assessment or facilitated with a CISA partner. The CPGs will be regularly updated, with a targeted revision cycle of every six to twelve months. As such, feedback is appreciated and can be submitted at https://www.github.com/cisa/cyber-performance-goals.

BENEFITS AND DELIVERY

The CPG assessment prioritizes by cost, complexity, and impact to inform stakeholders on strategies to implement and improve upon the five CSF functions. Each CPG outlines the security outcome, mitigation(s) that organizations should implement to achieve the outcome and reduce the impact of the TTPs or risk, the set or subset of assets to which organizations should apply the security practice, and example approaches to help organizations progress toward achievement of the performance goal based on input from CISA's collaborative stakeholder process.

CONTACT INFORMATION

For more information about the CPG program, contact CybersecurityPerformanceGoals@cisa.dhs.gov.