CYBERSECURITY PERFORMANCE GOALS:

A Roadmap For Critical Infrastructure

Tom Millar
US Cybersecurity and Infrastructure Security Agency (CISA)

Who am I? What are Cybersecurity Performance Goals (CPGs)?

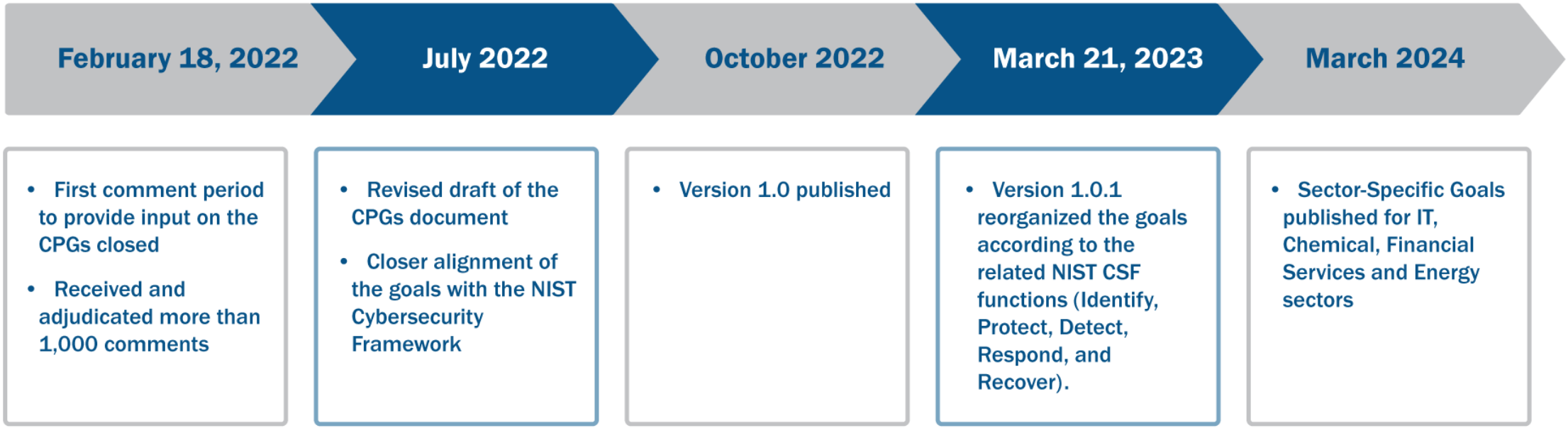
- I'm the Branch Chief for Cyber Resilience, in the Cybersecurity Division of CISA.
- My team covers a couple of high-intensity assessment services, training programs to teach others how to perform CISA-style assessments, and the CPGs.
- The CPGs are a common set of protections that all critical infrastructure entities should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.

Why Were The CPGs Created?

A need was identified for a consistent cybersecurity baseline for critical infrastructure, particularly environments with industrial control systems (ICS) / Operational Technology (OT).

The White House issued a National Security Memorandum on July 28, 2021, requiring that the Secretary of Homeland Security release a set of Cross-Sector CPGs one year from the date of the memorandum.

How The CPGs Were Developed



CISA gathered feedback from Critical Infrastructure Sector Coordinating Councils and worked directly with key ICS / OT subject-matter experts for guidance on goal development.

A wide range of participants were asked to provide feedback on the CPGs to ensure:

- **That partners and stakeholders had the opportunity to contribute input throughout the baseline CPG development process**
- **That the performance goals were as actionable and impactful as possible to the broadest stakeholder group.**

CPG CONTENT HIGHLIGHTS:

Supply Chain Incident Reporting

ID.SC-1
ID.SC-3

COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW

TTP OR RISK ADDRESSED:

Supply Chain Compromise (T1195, ICS T0862)

RECOMMENDED ACTION:

Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame, as determined by the organization.

CPG CONTENT HIGHLIGHTS:

Phishing-resistant MFA

PR.AC-7
PR.AC-1

COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM

TTP OR RISK ADDRESSED:
Brute Force (T1110). Remote Services - Remote Desktop Protocol (T1021.001). Remote Services - SSH (T1021.004). Valid Accounts (T1078, ICS T0859). External Remote Services (ICS T0822).

RECOMMENDED ACTION:
Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope). MFA options sorted by strength, high to low, are as follows:

- Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or PKI- based - see CISA guidance in “Resources”);
- If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used;
- MFA via SMS or voice only used when no other options are possible.

IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems.

OT: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible human-machine interfaces (HMIs).

FREE SERVICES AND REFERENCES: CISA Bad Practices

CPG CONTENT HIGHLIGHTS:

Limit OT Connections To Public Internet

PR.PT-4

COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** MEDIUM

TTP OR RISK ADDRESSED:
Active Scanning - Vulnerability Scanning (T1595.002)
Exploit Public-Facing Application (T1190, ICS T0819)
Exploitation of Remote Service (T1210, ICS T0866)
External Remote Services (T1133, ICS T0822)

RECOMMENDED ACTION:
No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (e.g., logging, MFA, mandatory access via proxy or other intermediary).

FREE SERVICES AND REFERENCES: Cyber Hygiene Services, "Stuff Off Search" Guide or email vulnerability@cisa.DHS.gov

CPG CONTENT HIGHLIGHTS:

Detecting Relevant Threats And TTPS

ID.RA-2,
ID.RA-3,
DE.CM-1

COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** HIGH

TTP OR RISK ADDRESSED:

Without the knowledge of relevant threats and ability to detect them, organizations risk that threat actors may exist in their networks undetected for long periods.

RECOMMENDED ACTION:

Organizations have documented a list of threats and cyber threat actor TTPs relevant to their organization (for example, based on industry, sectors, etc.), and have the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.

CPG CONTENT HIGHLIGHTS:

Incident Reporting

RS.CO-2
RS.CO-4

COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW

TTP OR RISK ADDRESSED:
Without timely incident reporting CISA and other groups are less able to assist affected organizations and lack critical insight into the broader threat landscape (such as whether a broader attack is occurring against a specific sector).

RECOMMENDED ACTION:
Organizations maintain codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g., state/federal regulators or SRMAs as required, ISAC/ISAO, as well as CISA).

Known incidents are reported to CISA and other necessary parties within time frames directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of
2022 (CIRCIA).

FREE SERVICES AND REFERENCES: Incident Reporting and/or contact report@cisa.gov or (888) 282-0870

CPG CONTENT HIGHLIGHTS:

Incident Planning And Preparedness

RC.RP-1
R.IP-9
PR.IP-10

COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** LOW

TTP OR RISK ADDRESSED:

Disruption to availability of an asset, service, or system

RECOMMENDED ACTION:

Develop, maintain, and execute plans to recover and restore to service business or mission-critical assets or systems that might be impacted by a cybersecurity incident

MEASURING ADOPTION OF THE CPGS:

What We Can Technically Observe

- **Email Security: Only 2% of organizations implement all three of the CPG's recommended technical practices (STARTTLS, DMARC and SPF).**
- **Strong and Agile Encryption: Most organizations still have multiple instances of outdated SSL/TLS, although the trend is positive.**
- **No Exploitable Services on the Internet: 80% of organizations have remediated all of their exploitable services.**

MEASURING ADOPTION OF THE CPGS:

What We Can Technically Observe

- **Mitigating Known Vulnerabilities: Most organizations show improvement, but few can claim 100% mitigation.**
- **Security.txt Usage: Unfortunately, this remains uncommon at most organizations.**
- **Limit OT Connections to the public Internet: Difficult to rigorously assess, but again, definitely not 100% adopted!**

MEASURING ADOPTION OF THE CPGS:

What We Have To Ask About

- **Most of the CPGs are about organizational practices rather than technically observable measures.**
- **Site assessments for critical infrastructure often come with additional data protections and are strictly voluntary.**
- **Self-Attestation CPGs include organizational practices like having IT and OT cybersecurity leadership, having IR plans in place, and vendor/supplier cybersecurity requirements.**

The Future, Part 1:

CPGs vs Cyber Incidents

- When CISA becomes the USA's national hub for Cybersecurity Incident Reporting for Critical Infrastructure (thanks to CIRCIA), we will potentially be able to compare frequency and severity of incidents (and TTPs) against the adoption of the CPGs by the same entity or sector
- This means we could do some rigorous analysis of practices vs incidence rate and impact – learning what really buys down risk without relying on anecdotal experience and intuition

The Future, Part 2:

Evolving The CPGs

- In the future, the CPGs might also include real "performance goals" – goals tied to specific time frames and tolerances, instead of just recommended practices
  - Think: "**Recover 95% of Operational Capacity Within 72 Hours of a Disruptive Cybersecurity Incident**"
- Future versions could also include goals for customer services and features – not just requiring phishing-resistant MFA, but ensuring it is available downstream
- More and more CPGs could be aimed at contract language practices rather than just requiring each organization to do things "on-prem"

How To Use The CPGs, Wherever You Are

The CPGs are all available from https://www.cisa.gov/cross-sector-cybersecurity-performance-goals - or just go to CISA.gov and search for CPGs.

You can also leverage CISA's Cybersecurity Evaluation Tool (CSET) to conduct your own CPG assessments: https://github.com/cisagov/cset/releases - or again, just use your favorite search engine and look for "CISA CSET"

Question Time!

Tom Millar

US Cybersecurity and Infrastructure Security Agency (CISA)

thomas.millar@cisa.dhs.gov