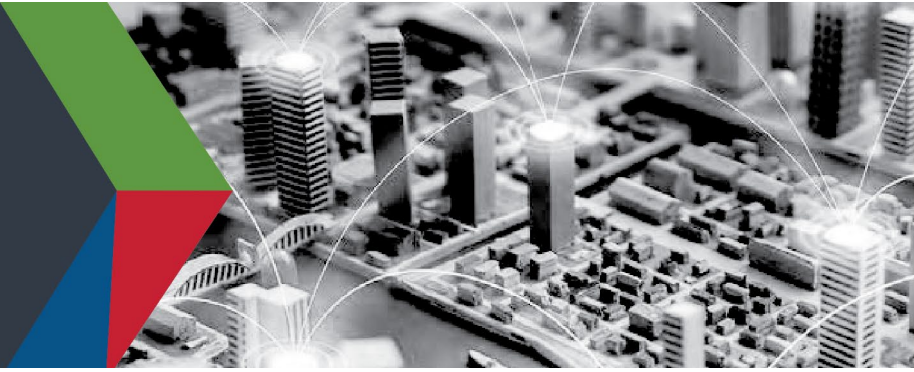

DEFEND TODAY, SECURE TOMORROW

SECURING INDUSTRIAL CONTROL SYSTEMS: A UNIFIED INITIATIVE

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) plays a unique role as the lead federal civilian agency responsible for advising critical infrastructure (CI) partners on how to manage industrial control systems (ICS) risk.

Fulfilling this role successfully requires both operational and strategic partnerships across the ICS community. Broadly, the ICS community includes all entities—government at all levels, the private sector, international partners, academia, and others—with equities in ICS security. CISA's focus on ICS security and commitment to collaborating with the ICS community is a vital part of its mission.

The CISA ICS strategy, *Securing Industrial Control Systems: A Unified Initiative FY 2019–2023*, focuses on working with CI owners and operators to build ICS security capabilities that directly empower ICS stakeholders to secure their operations against ICS threats. Through this initiative, we will also work to improve CISA's ability to anticipate, prioritize, and manage national-level ICS risk.

The intended audience for CISA's ICS strategy is the whole ICS community and all CISA partners who have an interest ICS security.

This fact sheet is a summary of the strategy document. You can find the full CISA ICS strategy at cisa.gov/ics.

CONNECT WITH US
www.cisa.gov/ics

For more information,
email cisamedia@cisa.dhs.gov

Linkedin.com/company/cisagov

@CISAgov | @cyber | @uscert_gov | @icscert_gov

Facebook.com/CISA

THE ICS CHALLENGE

Operational technologies are growing exponentially and migrating into domains not previously automated or connected to the internet (e.g., automobiles, medical devices, smart buildings and homes, pipelines, aviation).[1] Adding to the ICS risk topography is the deployment of 5G networks, which reduces reliance on traditional network routers, thus limiting the ability of security providers to monitor for and prevent malicious traffic.

The diverse ICS community comprises operational and strategic partnerships with equities in ICS security including: federal, state, and local governments; asset owners and operators; vendors; system integrators; international partners; and academic professionals in all 16 CI sectors. Every day, CISA works with our partners to help them identify, protect against, and detect cybersecurity threats and respond to and recover from significant incidents to both information technology and operational technology networks.

CISA'S ICS VISION

This initiative places significant emphasis on developing and implementing joint ICS security capabilities, mapping and identifying the degree to which specific national critical functions (NCFs) depend on ICS, and elevating and prioritizing ICS security around a unified, "One CISA" strategy. CISA's vision is to achieve a collective approach with industry and government that will:

- **Empower** the ICS community to defend itself;
- **Inform** ICS investments and proactive risk management of NCFs;
- **Unify** capabilities and resources of the Federal Government;
- **Move** to proactive ICS security; and
- **Drive** positive, sustainable, and measurable change to the ICS risk environment.

As CISA implements this initiative over the next several years, the ICS threat environment will surely evolve. CISA will adapt to changes in the environment and manage specific ICS risk management activities accordingly; the foundational pillars around which this initiative builds will endure.

Want more details? Listen to Director Krebs's remarks on CISA's ICS strategy at the June 2020 ICS Joint Working Group virtual meeting or read the full ICS strategy at cisa.gov/ics.

[1] More than 21 billion IoT devices are expected by 2025 (Source: *The future of IoT: 10 predictions about the Internet of Things*, https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html); https://www.us-cert.gov/ncas/tips/ST17-001