



POLICY BRIEF · ASPC-PB-021

# Trusted Digital Infrastructure and Cooperation

How can institutions frame digital cooperation around governance, prioritized risk reduction and shared responsibility?

---

**EVIDENCE-INFORMED ASPC ANALYSIS**

Supporting publication to ASPC-PP-002

August 2026 · 7-page edition

# Status, question and scope

## ASPC RESEARCH SYNTHESIS.

### Research question

How can institutions frame digital cooperation around governance, prioritized risk reduction and shared responsibility?

### Scope

Digital systems connect institutional capability to security, continuity, suppliers and public confidence. Cooperation requires governance as well as technical controls.

Evidence cutoff: August 21, 2026. Government findings, agency-reported information and ASPC analysis are distinguished throughout.

# Key findings

The reviewed sources support the following bounded findings.

- NIST CSF 2.0 organizes cybersecurity risk through Govern, Identify, Protect, Detect, Respond and Recover.
- CISA's voluntary cross-sector goals prioritize a limited set of practices intended to produce high-impact risk reduction.
- NIST supply-chain guidance calls for roles, supplier requirements and lifecycle risk management.

Findings are paraphrased from the cited official records. Source scope and date remain controlling.

# Evidence interpretation

## What the evidence establishes

- NIST CSF 2.0 organizes cybersecurity risk through Govern, Identify, Protect, Detect, Respond and Recover.
- CISA's voluntary cross-sector goals prioritize a limited set of practices intended to produce high-impact risk reduction.

## What requires judgment

Digital systems connect institutional capability to security, continuity, suppliers and public confidence. Cooperation requires governance as well as technical controls.

Application beyond the source setting is ASPC analysis and should be tested against the authority, capability, risk and conditions of the institutions involved.

# Implementation considerations

Implementation should connect responsibility, evidence and review.

- Establish governance, risk ownership, asset and dependency understanding before selecting tools.
- Use prioritized outcomes and sector context rather than treating every control as equally urgent.
- Include incident communication, recovery, supplier responsibilities and evidence of testing in agreements.

## Decision record

Document the responsible institution, required authority, resources, risks, measures, review date and basis for continuation, adjustment or conclusion.

# ASPC application and limitations

## Proposed application

- Establish governance, risk ownership, asset and dependency understanding before selecting tools.
- Use prioritized outcomes and sector context rather than treating every control as equally urgent.
- Include incident communication, recovery, supplier responsibilities and evidence of testing in agreements.

## Limitations

- This brief is not a security assessment, compliance determination or substitute for sector-specific technical expertise.

These applications are proposed by ASPC. Citation does not imply endorsement by any source institution.



# Trusted Digital Infrastructure and Cooperation

Supporting publication to ASPC-PP-002

## ASPC RELEVANCE

This research supports institutional stability and reliable international cooperation where capable institutions abroad can advance shared interests with the United States.

### NIST CSF 2.0

[Official source →](#)

### CISA Cross-Sector CPGs

[Official source →](#)

### NIST SP 1305

[Official source →](#)

**ASPC IS A U.S.-BASED STRATEGIC INITIATIVE AND NOT A UNITED STATES GOVERNMENT ENTITY.**

ASPC-PB-021 · Version 1.0 · August 2026