Office of Infrastructure Policy and Development (OIPD)

AI Task Force Briefing

Guam BEAD Program

NIST Cybersecurity Framework (CSF) 2.0

Digital / Cyber Posture and Readiness

Prepared in partnership with Pacific Alliance Group and Jacobs.

CONTEXT

Why This Matters

This work is being carried out under the direction of the Governor's Office of Infrastructure Policy and Development (OIPD), in direct support of Guam's federal BEAD Award.

Guam's digital infrastructure doesn't belong to any one branch or sector — it's the backbone the whole island runs on: community services, local business, tourism, contractors, military, and government alike.

Whole-of-Island Stakeholders

Residents, businesses, tourism, contractors, and military all depend on the same underlying digital ecosystem.

Federal Funding Readiness

Federal programs — including BEAD/ NTIA, DoD, DHS, DOI and other programs — increasingly condition funding on a demonstrated cybersecurity posture. This work builds that readiness.

Common Standard

NIST CSF 2.0 provides one consistent framework for assessing and improving posture — and aligns directly with NIST's AI Risk Management Framework, the standard guiding responsible AI adoption.

FOUNDATIONAL CONCEPT

What Is NIST CSF 2.0?

A framework for managing cybersecurity risk, built around six core functions:

GOVERN
Set strategy, roles, and risk management

IDENTIFY
Understand assets, business context, and risks

PROTECT
Put safeguards in place to reduce impact

DETECT
Spot cybersecurity events quickly

RESPOND
Contain incidents and communicate clearly

RECOVER
Restore services and improve after an incident

Why this matters for Guam

CSF 2.0 is the foundation of Guam's cyber and digital maturity — and the prerequisite for what comes next. NIST's AI Risk Management Framework, which will guide responsible AI adoption across the island, is built to run on this same governance and risk foundation. The CSF 2.0 work already underway isn't separate from Guam's future AI plans — it's the groundwork those plans depend on.

HOW WE GOT HERE

Phase 0 & Phase 1

Macro NIST CSF 2.0 Assessments

COMPLETE

Phase 0 – Macro-level Posture Assessment

- Macro-level review across all six NIST CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover
- Conducted workshops with line agencies across the GovGuam digital ecosystem
- Benchmarked against a maturity scale and cross-referenced with agency criticality
- Outcome: identified where cybersecurity risk concentrated across the ecosystem — surfacing GGWAN as the shared backbone warranting focused follow-on analysis
- Produced an initial NIST CSF 2.0 governance brief summarizing findings

Digital Ecosystem Readiness

ONGOING

Phase 1 — GGWAN Focused Deep-Dive

- Focused deep-dive scoped to GGWAN, the shared digital backbone, and BEAD-funded broadband assets
- Performing NIST Functions: Govern (oversight, supply chain, roles & responsibilities), Identify (asset inventory, risk assessment), and targeted Protect (physical access and environmental resilience of critical infrastructure)
- Includes mitigation development to support GGWAN using posture assessments
- Covers the agency impact/criticality framework and current- and future-state risk assessment
- Shifting from assessment to analysis and mitigation recommendations, aligned to both current-state posture and where the ecosystem needs to be

CURRENT STATUS

Where We're Driving Now

Actively working across all three in-scope NIST CSF 2.0 functions:

GOVERN

GV.OC, GV.RM, GV.RR, GV.PO, GV.OV, and GV.SC — **organizational context, risk management strategy, roles & responsibilities, policy, oversight, and supply chain risk management, built out with OIPD and OTECH – moving toward a new governance structure and organizational structure.**

IDENTIFY

ID.AM and ID.RA — **advancing the GGWAN asset inventory and risk assessment, covering both current-state and post-transformation risk – using a risk-based, tiered approach toward substantial coverage of the ecosystem to develop asset lifecycle, replacement-value analysis, and a finalized risk picture.**

PROTECT

PR.AA, PR.DS, and PR.IR – **Targeted physical access, data security, and technology infrastructure identification and resilience for critical infrastructure – the same baseline the BEAD NIST CSF 2.0 posture assessment is advancing on.**

RELEVANCE TO THIS TASK FORCE

How This Work Aligns With the Task Force

Alignment and sequencing considerations, by subcommittee:

Cybersecurity & Data Privacy

DIRECT

Core alignment. The governance and network maturity this work is building is what Agentic SOC, Next-Gen Zero Trust, and Continuous Identity Verification all require before they can be responsibly adopted.

AI Policies, Guidelines & Infrastructure

INFRASTRUCTURE

The subcommittee's 24-month statutory mandate assumes NIST CSF 2.0 alignment — this work is that alignment. Platform access expansion is downstream of the same governance work underway now.

AI Integration in the Workplace

SEQUENCING

Proposed pilots for high-volume, repetitive tasks depend on risk-vetted platforms and data that's been classified and risk-prioritized first — both are outputs of this phase's work.

HR/Profiling, Ethics/Deepfakes, and Accountability/Enforcement

FOUNDATIONAL

Not directly aligned today. A secure network and governance structure is the prerequisite for any of these three subcommittees' work to be meaningful.

AI Education & Social Media

MONITORING

No direct sequencing dependency today. As the governance and network foundation matures, we'll revisit whether secure-deployment considerations extend to classroom and public-facing AI tools.