Island Guardian FAQ

Cyber Readiness Initiative

Digital & Cyber Ecosystem Investment

for GovGuam's Defense-Relevant Line Agencies

Questions This Briefing Answers

THE CASE FOR ALIGNMENT

01 What immediate defense mission requirements does this investment address, and what demonstrates that it is more than a civilian IT modernization initiative? *(Slides 3-4)*

02 How does civilian digital/cyber infrastructure failure translate to military mission risk? *(Slides 5-8)*

03 How will this project improve military mission assurance, not just civilian IT? *(Slides 9-13)*

THE PLAN

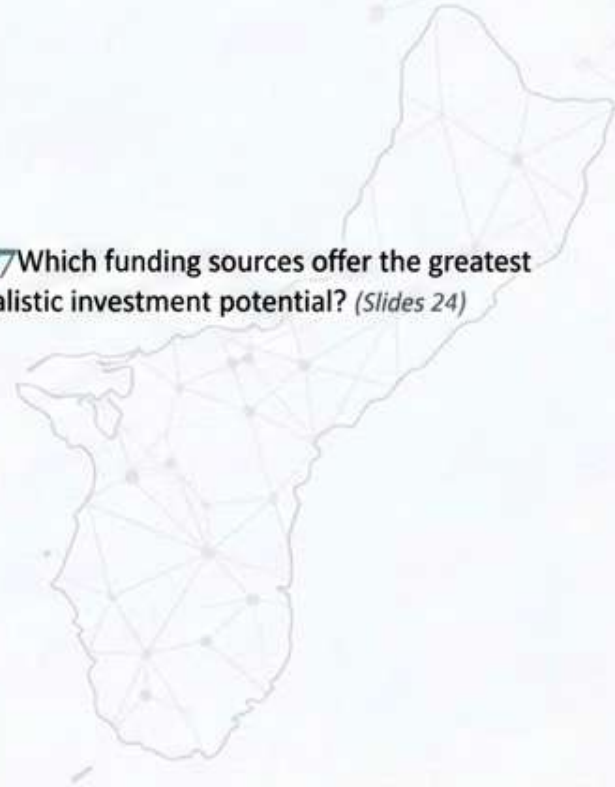
04 What's Guam's current Zero Trust maturity, what target state is required for defense-relevant agencies, and how does each investment phase close the highest-priority gaps? *(Slides 14-19)*

05 What's the investment phasing, allocation, and who in GovGuam will lead the execution of the investment? *(Slides 21-22)*

06 What's the first-12-months plan? *(Slides 22-23)*

THE FUNDING PATH

07 Which funding sources offer the greatest realistic investment potential? *(Slides 24)*



THE CORE RISK

Enhanced Integrated Air & Missile Defense (EIMD)/GDS runs on ordinary networks.

It operates across dozens of civilian systems—none of which are secured to the high standards required for critical military missions.

Every one of these already shares the same unsegmented backbone this investment secures.

This is why civilian network security and mission assurance are the same problem — not two.

VULNERABLE CIVILIAN DOMAINS INVOLVED

- Logistics & Cargo
- Medical Readiness
- Land & Infrastructure
- Housing
- Power & Water
- Emergency Response
- Roads & Transit
- Public Schools

Civilian Infrastructure Planning: A GAO-Documented Pattern

GAO has documented civilian infrastructure planning gaps across two prior Guam buildout phases. IT/cyber infrastructure has not yet been evaluated against that same pattern.

2008–2011 · OKINAWA BUILDUP

Civilian Infrastructure Inadequate After the Fact

REACTIVE

GAO found Guam's civilian infrastructure — power, water, roads, ports — inadequate for buildup demand. DoD funded only its own facilities; GovGuam was left responsible for the rest, largely discovered after construction was already underway.

2025 · EIAMD / GDS

Supporting-Facility Planning Still Deferred

REACTIVE — AGAIN

GAO found DoD hadn't yet determined GDS personnel requirements, so supporting-facility planning — housing, medical, utilities — couldn't be finalized. Assessment of civilian-infrastructure effects was deferred to a separate, still-pending study.

NOW · IT & CYBER

The One Domain Never Tested Against This Pattern

THE OPPORTUNITY

IT and cyber infrastructure has never been part of either GAO review — not because it was assessed and cleared, but because no one has looked yet. This is the one domain where planning can still happen before construction, not during it.

OIPD's $250M ask is the chance to be ahead of a Guam buildout for once — *not behind it and not discovering the gap after the concrete is already poured.*

Source: GAO-25-108187 (*Missile Defense: DOD Faces Support Challenges for Defense of Guam*, May 2025); GAO reports on the 2006–2014 Okinawa relocation buildup (GAO-08-722T, GAO-09-500R, GAO-09-653, GAO-10-90R, GAO-11-459R). *GAO has not assessed IT/cyber infrastructure specifically in either review — that gap is this analysis's observation, not a GAO finding.*

From Cyber Risk to Mission Risk

Three questions, in plain terms — what you need to know about each agency

Q1 — Could it be breached, and how far would the damage spread?

"Network & Infrastructure Exposure"

Four plain factors: how old/fragile the equipment is · how sensitive the systems it protects are · how many other agencies go down with it · how fast it can recover.

Q2 — If it's breached, who gets hurt, and how badly?

"Data Severity"

A system can be hard to breach but catastrophic if it is (tax records), or easy to breach but hold nothing sensitive. Rated Critical / High / Moderate / Minimal based on identity, financial, or health harm.

Q3 — Does it matter to the DoW mission — today's forces, or tomorrow's buildout?

"Mission Impact (National Defense Impact)" — the key DoW funding argument

PRESENCE

Andersen AFB, Naval Base, Camp Blaz, USCG — day-to-day sustainment, personnel, and military families relying on civilian services now.

PROGRAM (EIAMD/GDS)

Active DoW construction/modernization — new C2 sites, contractor workforce, and off-base housing demand moving through the island.

Line Agencies, by Mission Impact Class (22 of 31 with NDI Relevance)

Direct/Both — High
OTECH, CQA, DMA, GHS-OCD, DRT, DPHSS, DOA
Direct/Both/Indirect — Medium
GEC, GPD, DOL, DLM, Guam Recovery Office, DYA, DOAG, DPW, CSC
Direct/Indirect — Low
Governor's Office, BSP, DOE, DEPCOR, GMRO, AG

Why line agencies only: OIPD's $250M request is scoped to GovGuam's 31 line (executive branch) agencies directly influenced by GovGuam. This analysis focuses on the 16 with identified DoW-mission relevance.

The Dependency Chain

Line agencies driving mission risk — tagged by ongoing presence, active DoD programs, or both

OTECH✓

PRESENCE + PROGRAM

Office of Technology

Line · Cyber Tier 1 · Score 5.00 · Data CRITICAL

Network backbone — every GovGuam agency's digital function depends on it. Single point of failure.

Autonomous tie: Backbone serves ALL autonomous agencies as well as line agencies.

CQA✓

PRESENCE + PROGRAM

Customs & Quarantine Agency

Line · Cyber Tier 1 · Score 3.50

Customs/biosafety inspection at the port; interface criticality rising with crane upgrades + BSL-3/4 cargo.

Autonomous tie: Physically co-located with Port (PAG) and Airport (GIAA) — autonomous.

DPHSS

PRESENCE

Department of Public Health & Social Services

Line · Cyber Tier 2 · Data CRITICAL

Full population + military dependents; BSL-3/4 opening and hospital build reinforce Critical tier.

Autonomous tie: GMHA — only major civilian hospital, shared surge-care burden.

DOA

PRESENCE

Department of Administration

Line · Cyber Tier 1 · Data CRITICAL

Payroll/banking fraud risk; legacy AS400 system limits containment speed.

Autonomous tie: Feeds GGRF (autonomous, pension) and CSC (Line, personnel records — not autonomous).

DRT

PRESENCE

Department of Revenue & Taxation

Line · Cyber Tier 1 · Data CRITICAL

FTI breach forces mandatory federal data-access suspension; direct DoD-affiliated filer base.

Autonomous tie: No direct autonomous-agency tie — cascade risk flows to DPHSS and DOL, both line.

DMA✓

PRESENCE

Department of Military Affairs

Line · Statutory Defense Mission

Highest raw Defense Impact score of any line agency despite thin digital footprint — separate military networks.

Autonomous tie: None— operates on separate military networks.

✓ *= externally corroborated by CISA/NSA/FBI advisories or CRS.* **PRESENCE / PROGRAM / BOTH** *= which DoD mission context this agency's risk connects to (see slide 1)*

The Evidence, Line Agency by Line Agency

The 7 highest-priority line agencies — mission context (Presence/Program) and autonomous-agency ties flagged

Agency	Cyber Exposure	Data Sev.	Mission Context	Why It Matters to the DoD/Pacific Mission	Tie to Non-GovGuam Agencies (Autonomous)	Corrob.
OTECH	HIGH	CRITICAL	PRESENCE + PROGRAM	Every GovGuam agency's digital function depends on it	*ALL autonomous agencies (GPA, GWA, Port, Airport, GHC, GMHA, GGRF)*	✓
CQA	HIGH	MINIMAL	PRESENCE + PROGRAM	Customs/biosafety inspection; port throughput raises interface criticality	*Port (PAG) & Airport (GIAA) — physically co-located operations*	✓
DMA	ELEVATED	MINIMAL	PRESENCE	Highest raw Defense Impact score; separate military networks	*None identified — independent military networks*	✓
GHS-OCD	ELEVATED	MINIMAL	PRESENCE + PROGRAM	Explicit civil-military coordination role in disaster response	*Coordinates restoration across GPA, GWA, Port, Airport during disaster/conflict*	
DRT	HIGH	CRITICAL	PRESENCE	FTI breach forces mandatory federal data-access suspension	*None direct — cascades to DPHSS/DOL (both line)*	
DPHSS	HIGH	CRITICAL	PRESENCE	Full population + military dependents; BSL-3/4 opening, hospital build	*GMHA — only major civilian hospital, shared surge-care burden*	
DOA	HIGH	CRITICAL	PRESENCE	Payroll/banking fraud; legacy AS400 limits containment speed	*GGRF (pension) & CSC (personnel records) — cascade across both*	

PRESENCE *= existing installations/forces* **PROGRAM** *= EIAMD/GDS & active buildout* **BOTH** *= connects to both mission contexts*

Priority-Tier Hardening Is Phase 1 — Not the Whole Fix

Without network-wide segmentation, a breach anywhere on GGWAN can still reach the agencies this ask hardens

16 Priority-Tier Agencies

this $250M ask hardens directly

No segmentation between them

15 Remaining Agencies

unsegmented, partially unfunded by this ask

A bad actor doesn't need to breach a priority agency directly — any agency on an unsegmented network is a viable entry point to the ones that matter most.

PHASE 1

Priority-Tier Hardening

CURRENT ASK · $250M

Segmentation, IAM/MFA, and monitoring for the 16 highest-priority line agencies — the evidence base this deck presents.

PHASE 2

Network-Wide Segmentation & Zero Trust

CLOSES THE GAP

Extends segmentation and Zero Trust architecture across the remaining 15 agencies — closes the lateral-movement path Phase 1 alone cannot.

PHASE 3

Continued Capital Investment

LONGER HORIZON

Legacy system replacement, facility investment, and sustained capital renewal across the full digital ecosystem.

Phasing shown here is illustrative sequencing, not a committed schedule or budget — pending team validation, consistent with the rest of this program's planning materials.

Bottom Line Up Front

Mission-Critical Assessment

OIPD's $250M digital/cyber investment is not a civilian IT request.

It protects the same network, the same population, and the same dollars that already carry EIAMD/ GDS mission execution on Guam.

Why This Investment Is Required

01

Scope & Mission Risk

All 16 of GovGuam's line agencies are in scope. The highest-priority 7 carry the most acute, most-evidenced DoW-mission risk today — proof of concept for the full ecosystem, not the limit of it.

02

Infrastructure Dependencies

The dependencies are not hypothetical: shared data already bridges into GPA, GWA, the Port, and the Airport, and a majority off-base – now school-age – military population already runs on this same backbone.

03

Steady-State & Buildout Posture

Both steady-state posture and active-buildout execution — construction uptime, permitting, contractor retention — depend on the same fix.

04

Federal Compliance Triggers

Federal compliance failure moves at the same speed as a cyberattack: an IRS, FBI/DOJ, or HHS-triggered suspension would halt services DoW personnel and their families already rely on.

What This Investment Buys the Mission

Current exposure → funded intervention → concrete mission-assurance outcome, for the 7 highest-priority of OIPD's priority tier 16 line agencies in scope

Agency	Current Exposure	Funded Intervention	Mission Assurance Outcome
OTECH	Tier 1 · Score 5.00 — sole SPOF	New Tier III facility + Zero Trust network backbone, redundant fiber paths	Backbone survives single-component failure — sustains connectivity for EIAMD/GDS C2 sites and every other agency during an outage or attack.
CQA	Tier 1 · Score 3.50	OT/ICS segmentation, IAM/MFA, physical hardening at inspection points	Customs/biosafety clearance continues without disruption — protects Port/Airport cargo flow supporting base logistics and buildout materiel.
GHS-OCD	Tier 2 · Score 2.60	Segmentation, logging, coordination-system hardening	Disaster/contingency coordination with GPA, GWA, Port, Airport stays functional during a regional conflict or major storm — the exact scenario mission assurance exists for.
DRT	Tier 1 · Data CRITICAL	Pub 1075-compliant segmentation, encryption, MFA	Prevents IRS-mandated suspension of DRT's federal data-sharing access — keeps tax processing uninterrupted for a filer base that includes DoD-affiliated personnel.
DPHSS	Tier 2 · Data CRITICAL	HIPAA-aligned hardening, rapid detection/ response infrastructure	Sustains military-dependent surge-care capacity and keeps the new BSL-3 lab's OpenELIS/eCR diagnostic-reporting feeds online during a health emergency or cyberattack.
DOA	Tier 1 · Data CRITICAL	Segmentation, IAM/MFA, outdated legacy computer system remediation	Protects payroll continuity for the GovGuam workforce, including personnel supporting DoD-adjacent contracts — stops fraud cascading into GGRF/CSC.
DMA	Tier 3 · Score 2.00	Baseline hardening, compliance documentation, coordination interface	Secures the one line agency with a direct statutory defense mission, even though its core networks stay separate — closes the last gap in the ecosystem.

Scope: *These 7 of 16 priority tier line agencies are OIPD's highest-priority, most-evidenced tier— not the total ask. The remaining 15-line agencies, at various investment levels, are covered under the same $250M request.*

Note: *Outcomes above are this analysis's projected effect of the funded intervention.*

The Hidden Dependencies

Where civilian systems quietly carry military weight — and what breaks if they don't

The Data Bridge to Critical Infrastructure

A line agency doesn't need a shared network with GPA, GWA, the Port, or the Airport to put them at risk – a data relationship is enough. Land records can carry utility easement details. Inspection staff can authenticate onto a co-located agency's network. Environmental data can identify specific weak points. Comprise the agency holding the data, and exposure follows it to whichever critical infrastructure agency depends on it.

Hidden because: *Reads as routine data-sharing. It's risk transfer – critical infrastructure inherits exposure from whoever hold data about it, wired together or not.*

The Shared Health-Security Pipeline

The BSL-3 lab and DPHSS's diagnostic pipeline aren't reporting infrastructure – they're Guam's early-warning system for disease outbreaks. The surge construction workforce and the resident community run through the exact same detection pipeline; a disruption delays outbreak detection for whichever population needs it first; community or contractor, without distinction.

Hidden because: *Reads as "healthcare IT" or a compliance checkbox. It's the shared health-security backbone protecting the buildout workforce and the people already living here alike.*

The Off-Base Majority

60%+ of military personnel already live off-base — Guam inverts the typical ratio due to on-base capacity limits — growing from 17,000 to 24,000 active-duty by 2033. That dependency is now extending into schools: DoDEA has already toured for GDOE campuses to prepare for military-dependent student overflow.

Hidden because: *Reads as "civilian services" and "local schools." For most military families on Guam, GovGuam's services – and soon, GovGuams's classrooms - already are their services.*

The DRT Cascade

A breach at the DRT isn't a routine IT incident – DRT holds FTI, and IRS requires mandatory suspension of federal data access following a breach. That suspension doesn't stay contained to DRT: the underlying cost model shows it directly binding two or more agencies – both of which rely on DRT data to verify resident benefit eligibility. One breach, three agencies down.

Hidden because: *This gets filed as a single-IT risk. It's a documented three-agency cascade with a federal compliance trigger attached – not an assumption layered on top of the analysis.*

OPEN **DPW — Traffic & Evacuation Digital Infrastructure**

Two distinct threads, different confidence: *(1) DPW's road systems plausibly double as evacuation-routing infrastructure — Typhoon Mawar (2023) damaged civilian and military infrastructure simultaneously — but no source yet ties DPW's current digital systems to evacuation planning specifically. (2) Forward-looking: DPW's road-corridor MILCON overlap makes it a plausible future host for an Intelligent Transportation System to manage buildout-era traffic — a new networked surface that should be secured by design from inception, not retrofitted. Neither claim is established scope; both are worth validating before this goes further.*

Four Dimensions of Steady-State Mission Assurance

Continuity of Operations

FROM: OTECH single point of failure; no redundant paths

TO: Tier III facility, dual diverse fiber, Zero Trust segmentation

Civilian network backbone keeps functioning through a component failure, natural disaster, or attack — sustaining connectivity for EIAMD/GDS C2 sites and every dependent agency, not just OTECH itself.

Threat Detection & Response Speed

FROM: No islandwide SIEM/logging; ad hoc, siloed monitoring

TO: Centralized SIEM/logging, managed SOC/MDR across Critical-tier agencies

Time to detect and respond to an intrusion drops from days/undetected to continuous, correlated monitoring — directly addresses the exact Volt Typhoon pre-positioning pattern CISA/NSA/FBI have documented against Guam's infrastructure.

Data Integrity & Compliance

FROM: DRT/GPD/DPHSS exposed to Pub 1075, CJIS, HIPAA non-compliance

TO: Compliance-aligned segmentation, encryption, MFA, audit logging

Prevents federal agencies (IRS, FBI/DOJ, HHS) from suspending GovGuam's data-sharing access — an administrative failure that would halt services DoW personnel and their families rely on just as fast as a cyberattack would.

Workforce & Sustainment

FROM: Entirely contractor-dependent; no GovGuam-operated capability

TO: 4–6 GovGuam FTEs by Year 3, phased transition, managed-service backstop

Mission assurance doesn't expire when federal funding does — Guam retains the people and processes to sustain the posture independently, which is what makes this a durable investment rather than a temporary fix.

Tactical Assurance During Active Buildout

Steady-state assurance protects the mission at rest. This protects the mission in motion — while EIAMD/GDS is under construction

Construction Uptime & Logistics Throughput

CQA

From: *Customs/biosafety inspection unsegmented; Tier 1 exposure rising with crane upgrades*

To: *OT/ICS segmentation, IAM/MFA at inspection points*

Material and cargo clearance keeps moving — fewer schedule slips waiting on customs processing for buildout materiel at the Port and Airport.

Permitting & Regulatory Velocity

DPW

From: *Near-zero hardening; road-corridor systems overlap pending NDAA MILCON scope*

To: *Baseline segmentation, reliable digital permitting/inspection systems*

Fewer construction stand-downs caused by permit-system outages or inspection backlogs on roads and corridors shared with MILCON work.

Contractor & Workforce Quality of Life

DLM · DPHSS

From: *Land/property records (off-base housing) and healthcare systems unsegmented, Moderate–Critical exposure*

To: *Segmentation, IAM/MFA, sustained system availability*

Reliable housing-title processing and healthcare access for the surge contractor population — a retention and productivity factor, not just a civilian benefit.

Contingency Resilience During Active Construction

GHS-OCD

From: *Coordination systems exposed; untested under simultaneous construction-phase and disaster-response load*

To: *Segmentation, logging, hardened coordination interface*

Emergency response stays functional even with an active work site and surge population on the ground during a typhoon or incident.

Current Zero Trust Maturity Posture

All five pillars are at the Traditional stage. This is the expected position for a territorial government without a funded, governed Zero Trust program.

OVERALL MATURITY

0.27

Traditional — of a possible 3.00

36-MONTH TARGET

1.45

Initial — recommended, not maximal

FUNCTIONS AT 0.00

21 of 37

Rated Traditional with no partial credit

CRITICAL FINDINGS

14

Of 37 assessed functions

Pillar	Current	Score	Target	Gap	Critical	At 0.00
Identity	Traditional	**0.29**	Initial (1.71)	**+1.43**	**4**	4 of 7
Devices	Traditional	**0.36**	Initial (1.64)	**+1.29**	**2**	3 of 7
Networks	Traditional	**0.29**	Initial (1.36)	**+1.07**	**1**	4 of 7
Applications & Workloads	Traditional	**0.19**	Initial (1.19)	**+1.00**	**3**	5 of 8
Data	Traditional	**0.25**	Initial (1.38)	**+1.13**	**4**	5 of 8
ENTERPRISE OVERALL	**Traditional**	**0.27**	**Initial (1.45)**	**+1.18**	**14**	**21 of 37**

Current Maturity Against The Recommended Mission Target

The Identity gap is the largest by design: access control governs every other control, so it should move furthest and fastest.

Reading the scale

Traditional

0 — where all five pillars sit today

Initial

1 — the recommended 36-month target

Advanced

2 — Identity only, in its highest-value functions

Optimal

3 — not recommended for Guam now

Why not Optimal? Pursuing Optimal across all pillars needs specialist staffing the territorial labour market cannot supply and recurring funding not yet identified. An evenly enforced Initial posture reduces more risk than an unevenly operated Advanced one.

What The Averages Conceal

A pillar average is a comparison device. Three imbalances carry more risk than their arithmetic contribution suggests.

1 Devices scores highest but narrowly

The 0.36 average rests on one function: endpoint detection at 1.00. Coverage of servers, autonomous agency endpoints, and operational technology is unverified, and alerts are not monitored outside business hours.

A capable tool nobody is watching at 2 a.m. does not deliver the outcome the score implies.

2 Traffic encryption at 1.00 hides a missing inventory

Public-facing encryption lifts the score. Internally, cleartext protocols persist and certificate expiries have already caused outages, the reliable symptom of no enterprise certificate inventory.

The score reflects the perimeter; the risk sits inside it.

3 Data encryption at 1.00 is inherited, not managed

Encryption at rest is largely a platform default. There is no key management standard, no view of where keys and secrets are held, and credentials are embedded in scripts and configuration files.

Encryption at rest does not defend against the attack path that threatens the data.

OTECH (GGWAN) — Zero Trust Maturity: Current vs. Target

CISA ZTMM v2.0 mapped from OTECH's NIST CSF assessment findings

BLUF:
OTECH sits at Traditional on all 8 measurable pillars — nothing has moved yet. The small red shape and the large teal shape don't overlap anywhere.

Highest-severity evidence, by pillar

Identity

Shared accounts and inconsistent password hygiene; MFA not fully enforced.

Networks

Flat network; daisy-chained unmanaged switches; no downstream firewalls.

Data

No classification, encryption, or DLP requirements defined for sensitive data.

Visibility & Analytics

No centralized SIEM/SOC; no formal alert thresholds or correlation rules.

Governance

No dedicated cybersecurity team; cyber risk not in enterprise risk management.

Applications & Workloads has no corresponding CSF evidence in either assessment and is not scored — not inferred.

Current State — Traditional (all 8)

Target — Advanced

Source: OTECH NIST CSF assessment (Identify/Protect/Detect/Respond/Recover/Govern, including sub-category detail), mapped to CISA ZTMM v2.0 by this analysis — not an independent ZTMM survey.

Zero Trust Maturity Across Line Agencies: A Sampling

CISA ZTMM v2.0 mapped from each agency's own NIST CSF assessment findings

Source: OTECH NIST CSF assessment (Identify/Protect/Detect/Respond/Recover/Govern, including sub-category detail), mapped to CISA ZTMM v2.0 by this analysis — not an independent ZTMM survey.

What These Gaps Mean In Practice

Five scenarios follow from the assessment. They are described in terms of government services, not technical controls.

		Likelihood	Impact
1	**Territory-wide ransomware from one phished administrator** Permanent, unbrokered, phishable privileged access plus permissive internal reachability. Backup integrity and restoration are unverified.	High	Severe
2	**IT compromise propagating to power, water, and port systems** Operational technology at utility and transportation entities is not demonstrably isolated from enterprise IT.	Moderate-High	Severe
3	**Undetected exfiltration of citizen records** Local application credentials, little application logging, accumulated broad access, and no export monitoring.	Moderate	Severe
4	**Internet-facing service compromise** Protection set by hosting arrangement rather than standard. This is the pattern of the May 2026 incident that disrupted GovGuam public websites.	High	Major
5	**Typhoon and cyber incident at the same time** Unverified agency redundancy, untested failover, no evidence of off-island backup in a jurisdiction where both hazards are live.	Moderate	Severe

Likelihood · Impact assessed against mission consequence for the island, not technical severity alone.

Escalating Investment by Priority

Island Guardian — Investment Phased Request, Years 1–5

Capital – Hardware & Software

Installation & Deployment

PMO / Governance / Oversight

Implementation Support

Operational Workforce & Sustainment

Year 1 – Foundation ($37M)
Program stands up: PMO governance, OTECH facility design and long-lead procurement begin, initial capital investment on the highest-priority network infrastructure.

Year 2 – Peak Build ($65M)
Heaviest year of investment. OTECH facility construction accelerates, network hardening rolls out across the highest risk agencies, PMO reaches full operating capacity, and implementation support (SOPs, legacy data migration, initial training) begins as the first agencies transition.

Year 3 – Sustained Execution ($59M)
Still capital-intensive but past the peak. Facility work nears completion, remaining agency hardening continues, and the program's center of gravity starts shifting toward implementation and early workforce transition.

Year 4 – Transition ($35M)
Capital spending tapers sharply as major construction and network buildout wind down. Investment shifts toward implementation support, training, and standing up GovGuam's operational workforce.

Year 5 – Steady State ($23M)
Lowest-investment year. Remaining work is software licensing renewal, final implementation support, and full transition to GovGuam operated sustainment – the program moves from build to run mode.

Minimum viable first investment: a defined Year 1 launch tranche within the $37M Foundation phase, funding PMO stand-up, facility planning, and initial priority-agency network hardening.

Cost Escalation by Delivery Exposure

COST BASIS | WORKING

Working assumptions distinguish Guam-driven delivery costs from nationally priced services and software.

	COST ELEMENT	WORKING FACTOR	COST DRIVER / APPLICATION
1	Facility / physical infrastructure	2.75x	Construction labor, freight, site work, permitting, redundant power, and limited local capacity
2	Network hardware / field infrastructure	Split Factor	Apply Guam uplift to shipped, installed, and field-supported components; use national pricing for equipment where applicable
3	Software licensing / remote services	National Rates	IAM, SIEM, MDR, SaaS, and cloud services are generally enterprise-priced; exclude a blanket island multiplier
4	Installation & deployment	1.5–2.5x	Site labor, mobilization, integration, testing, travel, staging, and potential remobilization between locations
5	PMO / governance / oversight	Blended Basis	Mainland professional-services rates plus a targeted allowance for Guam presence, travel, coordination, and delivery risk
6	Implementation support	1.5–2.5x Blended	Remote design and documentation at base rates; onsite migration, go-live support, training, and adoption receive an uplift
7	Operations / sustainment	Split Factor	Adjust local technicians, vehicles, spares, and dispatch; retain national rates for virtual SOC/MDR and remote managed services

CORE PRINCIPLE

Apply escalation where Guam drives the cost—not as a blanket island multiplier.

PMO anchor: mainland-led execution + targeted Guam delivery allowance.

The Foundation Already Laid

This program isn't starting from zero — OIPD has already completed the groundwork the next 12 months builds on

NIST CSF Posture Assessment

COMPLETE

Cybersecurity Framework 2.0 assessment scoped and executed across GovGuam agencies — current-state maturity now documented, not estimated.

GGWAN Asset Inventory

SUBSTANTIALLY COMPLETE

Critical assets are inventoried with enough specificity to act now, including which systems are beyond service life or running firmware that can’t meet current cybersecurity standards. Other assets related to service reliability and resilience like cabling condition and power distribution/backup continue to be mapped in parallel.

Consequence-Driven Cyber Informed Engineering Assessment (CCE Threat & Resilience Study)

ONGOING

A consequence-driven methodology, run continuously – working backward fr0m the mission outcomes that matter most to identify which civilian systems could cause them. Findings directly reprioritize where hardening happens first, not a one-time snapshot.

Lifecycle & Supply Chain Assessment

ONGOING

Existing hardware/software inventory assessed for end-of-life status and vendor viability, surfacing supply-chain risk across critical systems. In parallel, OIPD is developing improved internal processes and external vendor-management strategies to sustain assets and manage risk going forward.

This is why the next 12 months can move directly into hardening and procurement rather than starting with another assessment cycle.

The Next 12 Months, By Workstream

OTECH leads on two fronts simultaneously — the new facility and hardening what exists today — before other agencies scale up

OTECH — Facility (Housing)

START NOW

- Finalize facility requirements & programming
- Evaluate build/buy/lease/hybrid models

OTECH — Network Hardening

START NOW

- Complete backbone segmentation design
- Pilot Zero Trust identity controls

Priority-Tier Agency Hardening

- Finalize segmentation designs
- Begin IAM/MFA: DRT, DOA, DPHSS

Assessment & Governance Wrap-Up

- Close remaining CSF gaps
- Stand up PMO governance

Federal / EAC Coordination

- Formalize EAC/OLDCC reporting cadence
- Pursue BEAD non-deployment waiver

Workforce & Sustainment Planning

- Define FTE roles & recruiting plan
- Scope managed SOC/MDR contract

OTECH's two tracks dominate Q1 effort, then taper as agency-level hardening scales up to take their place.

Tasks are illustrative and high-level, pending team validation. START NOW = work that should begin in Q1 regardless of when the broader $250M request is finalized.

Funding Sources, Ranked by Investment Potential

Prioritized scalable, mission-aligned funding pathways

Confirmed pathway | Assumption-dependent | Strategic / uncertain | Minor / unconfirmed

1 NTIA BEAD Non-Deployment Savings

OIPD-administered

ASSUMPTION-DEPENDENT

Guam's total BEAD allocation exceeds $156M with $130M available in non-deployment funds. Requires NTIA's pending non-deployment guidance to include cybersecurity, or a written waiver — Guam's insular profile (waived cost-share, high-cost/remote burden) supports the case, especially with EAC/DoD backing.

Assumes cybersecurity/network security becomes an eligible BEAD non-deployment use via territorial waiver

$130M+

2 OLDCC — DCIP / EAC Grant Authority

Existing relationship

CONFIRMED PATHWAY

FY26 DCIP: $230M available nationally, competitive, capped at $20M per award — facility-scale asks need phasing across cycles. Broader OLDCC grant authority (non-DCIP) more flexible. Already the active relationship via CDLO-26-003 — most certain source on this list.

~$20M/award cap

3 DoD Service / INDOPACOM Direct Funding

EIAMD/GDS-tied

STRATEGIC / UNCERTAIN

No public NOFO — requires DoD to formally own part of the cost as mission-necessary. Highest theoretical ceiling given EIAMD/GDS budget scale. Best lever for reinforcing Row 1: DoD/JTF-M mission-relevance statements give NTIA institutional cover to grant the BEAD waiver.

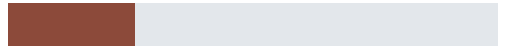
Uncertain ceiling

4 HHS/CDC — Public Health Infrastructure

DPHSS-tied

UNCONFIRMED SCALE

Plausible fit given BSL-3/4 biodefense adjacency and DPHSS's Critical data severity — program funding levels not yet verified. Narrow, agency-specific; not a program-scale contributor without further research.



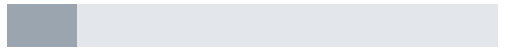
Unconfirmed

5 DOJ — Bureau of Justice Assistance (Byrne JAG)

GPD/CJIS-tied

MINOR / FORMULA-BASED

Formula-based territorial allocation, typically modest. Useful for GPD's specific CJIS-compliance line item only, not a material program-level contributor.



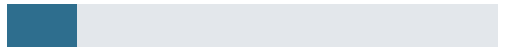
Low single digits ($M)

6 FEMA/CISA — SLCGP

Cost-share waived for Guam

MINOR — MATCH WAIVED

National SLCGP funding fell to $91.75M in FY25 (from $374M in FY23); Guam's 0.25% territorial base allocation is small in absolute terms. Federally waived cost-share means whatever is awarded costs GovGuam nothing in match — worth pursuing for a discrete sub-component, not program scale.



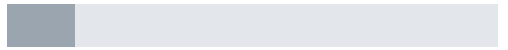
Low single digits ($M)

7 DOL — Workforce & Training Grants

Implementation Support-tied

MINOR / INDIRECT

Weakest mapping of the group — relevant only to the training/change-management slice of Implementation Support, not treated as a capital contributor.



Smallest, indirect

Ranking reflects realistic achievable scale, not category fit alone — several categorical "best fits" (SLCGP, Byrne JAG) are structurally small for a program at this scale. Pre-Decisional.

REFERENCE

Acronym & Term Glossary

Every acronym and defined term used across this deck, in one place

BSL-3 Biosafety Level 3 (lab biocontainment rating)

C2 Command and Control

CISA Cybersecurity & Infrastructure Security Agency (DHS)

CJIS Criminal Justice Information Services (FBI security policy)

CQA Customs & Quarantine Agency (Guam)

CSC Civil Service Commission (Guam)

DLM Department of Land Management (Guam)

DMA Department of Military Affairs (Guam)

DoW Department of War

DoDEA DoD Education Activity (runs on-base military schools)

DOA Department of Administration (Guam)

DOJ Department of Justice

DPHSS Dept. of Public Health & Social Services (Guam)

DPW Department of Public Works (Guam)

DRT Department of Revenue & Taxation (Guam)

eCR Electronic Case Reporting (disease surveillance)

EIAMD Enhanced Integrated Air & Missile Defense system

FBI Federal Bureau of Investigation

FTE Full-Time Employee

FTI Federal Tax Information

GDOE Guam Department of Education

GDS Guam Defense System (same buildout as EIAMD)

GGRF Government of Guam Retirement Fund

GHS-OCD Guam Homeland Security / Office of Civil Defense

GPA Guam Power Authority

GPD Guam Police Department

GWA Guam Waterworks Authority

HHS U.S. Dept. of Health & Human Services

HIPAA Health Insurance Portability & Accountability Act

IAM Identity & Access Management

ICS Industrial Control Systems

IRS Internal Revenue Service

MDR Managed Detection & Response

MFA Multi-Factor Authentication

MILCON Military Construction

NDAA National Defense Authorization Act

NSA National Security Agency

OIPD Office of Infrastructure Policy & Development (Guam)

OpenELIS Open-source lab information system (diagnostics)

OT Operational Technology

OTECH Office of Technology (Government of Guam)

Pub 1075 IRS Publication 1075 (FTI safeguarding standard)

SIEM Security Information & Event Management

SOC Security Operations Center

SPOF Single Point of Failure