**ISLAND SECURITY POLICY INSTITUTE**

ispiglobal.com · ISPIGlobal@proton.me · (808) 999-0544

**WHITE PAPER**

# Organizational Insider Threat Assessment Framework for Island and Small-State Communities

*A Practitioner-Grounded Detection and Response Architecture for Organizations Mainstream Frameworks Cannot Serve*

---

**Research Pillar:** Insider Threat & Workplace Security Policy

**Document Type:** White Paper

**Author:** Warren Pulley, Founder & Executive Director

**Institution:** Island Security Policy Institute — Honolulu, Hawai‘i

**Published:** 2026

**Contact:** ISPIGlobal@proton.me · (808) 999-0544 · ispiglobal.com

**Keywords:** insider threat framework island communities, behavioral threat assessment Hawaii, BTAM small organizations, insider threat detection Pacific Islands, organizational security island states, workplace security framework Hawaii, CERT insider threat island, DHS insider threat small organizations

---

**RESEARCH INDEPENDENCE STATEMENT**

*The Island Security Policy Institute is a nonprofit, nonpartisan research organization registered in the State of Hawaii. This publication represents ISPI's independent research and policy analysis. Views expressed do not necessarily reflect the position of any funder, sponsor, or affiliated organization. ISPI maintains full editorial independence on all research outputs. Commissioning clients do not influence ISPI's research conclusions, policy recommendations, or published findings. Full institutional credential documentation is available to qualified government agencies, foundations, and institutional partners upon formal request.*

EXECUTIVE SUMMARY

- **Standard insider threat detection frameworks — including the Carnegie Mellon CERT Common Sense Guide and DHS Insider Threat Program guidance — assume organizational scale, institutional distance, and anonymous reporting infrastructure that small island-state organizations structurally cannot achieve.**
- **The social cost of formal threat reporting in small island-state organizations is demonstrably higher than in large continental organizations, producing systematic underreporting of behavioral warning signs that is the defining pattern of insider threat failure in island communities.**
- **ISPI's four-component Organizational Insider Threat Assessment Framework addresses the structural gaps: calibrated behavioral baselines, third-party assessment pathways, access governance compensating controls, and graduated response protocols for sole-provider workforces.**
- **Pilot implementation of island-specific frameworks in Hawaii and Pacific Island organizations demonstrates measurably improved detection rates compared to standard framework implementation.**

In 2023, a Pacific Island territory health department discovered that a network administrator had been copying patient records to a personal cloud storage account for fourteen months. The administrator had full system access — because in a twelve-person IT department, there was no one else to grant access to. The segregation of duties that cybersecurity frameworks prescribe as the primary defense against privileged insider threat did not exist. One person was simultaneously the network administrator, the backup administrator, and the access auditor.[1]

This case illustrates the fundamental incompatibility between digital insider threat frameworks designed for large enterprise environments and the IT governance realities of small island-state organizations. ISPI's analysis of insider threat incidents across Hawaii and Pacific Island organizations identifies this incompatibility as the defining pattern — and proposes a practitioner-grounded assessment framework specifically designed for the organizational and social environments where that failure most consistently occurs.

## I. The Scale Assumption Problem

The foundational assumption embedded in every major insider threat detection framework is organizational scale. The Carnegie Mellon CERT Common Sense Guide to Mitigating Insider Threats — the most widely cited practitioner framework in the field — prescribes detection practices that require dedicated

security personnel, formal HR investigation functions, anonymous tip lines, segregated access administration, and the institutional distance between colleagues that makes behavioral monitoring socially feasible.[2]

A 22-person county water authority on a Pacific Island territory does not have dedicated security personnel. A 45-person resort in rural Hawaii does not have a formal HR investigation function. A 12-person government health department on a neighboring island does not have an anonymous tip line that is meaningfully anonymous — because in an organization of 12 people, the identity of any reporter is immediately inferable. These organizations cannot implement standard frameworks because the frameworks were not designed for them.

### The Social Cost of Reporting

The social cost of formal threat reporting in small island-state organizations — where professional and personal relationships overlap substantially across the entire career — is sufficiently high that underreporting of behavioral warning signs is the norm rather than the exception. ISPI's practitioner analysis of more than 2,400 documented threat assessments confirms this pattern across sectors.[3]

## II. The Island-State Insider Threat Environment

The defining characteristic of small island-state organizational environments — from the perspective of insider threat detection — is the overlap between professional and personal social networks. In a small Pacific Island territory government agency, a Hawaii county office, or a rural island resort, the employees who work together also attend the same churches, coach the same youth sports teams, and share family connections that run multiple generations deep through the same community.

> **ISPI's practitioner analysis of documented insider threat incidents in small island-state organizations consistently identifies the social reporting barrier as the primary mechanism through which behavioral warning signs go unaddressed — not insufficient detection capability, but social architecture that makes detection capability inoperative.**

### The Workforce Irreplaceability Constraint

In a continental organization, an employee whose insider threat indicators trigger concern can be suspended or terminated with confidence that operational capacity will be restored through replacement hiring. In a small island organization — particularly in healthcare, government, or critical infrastructure — the subject of concern may be the only licensed clinical nurse available to the ICU, the only IT administrator who knows the legacy system, or the only port operations manager with required certifications.[4]

## III. The ISPI Four-Component Framework

### Component 1: Calibrated Behavioral Baseline Assessment

Standard behavioral indicator training applies continental organizational norms to island community organizational contexts. ISPI's Component 1 develops behavioral baselines specific to the organizational and cultural environment — not the generic baseline embedded in BTAM training curricula calibrated on North American continental data. The calibration process involves cultural baseline calibration, organizational baseline calibration, and community context calibration across three dimensions unique to Pacific Island and Native Hawaiian organizational environments.

### Component 2: Third-Party Assessment Pathways

Anonymous internal tip lines are not meaningfully anonymous in small organizational environments of 15 to 50 employees. ISPI's Component 2 routes behavioral concerns to a qualified external assessor operating entirely outside the organizational social network — removing the social cost from the reporting decision by removing the reporter from the organizational consequences of reporting.

### Component 3: Access Governance Compensating Controls

Where segregation of duties is structurally impossible, compensating controls provide meaningful detection capability: third-party access auditing, automated anomaly detection, peer oversight protocols, and external managed security service arrangements calibrated for small island organizational budgets.[5]

### Component 4: Graduated Response Protocols

Standard detect-assess-remove response sequences do not account for workforce irreplaceability constraints. ISPI's Component 4 provides a graduated response architecture across four risk levels — observation, concern, alert, and response — with workforce continuity planning required before any personnel action at the response level.

> "*The most consequential insider threat failures in island organizations are not detection failures. They are reporting failures — produced by a social architecture that makes detection capability inoperative.*"

## IV. Sector-Specific Adaptations

ISPI's framework includes specific adaptations for island government agencies (political relationship mapping), island healthcare organizations (clinical

continuity assessment before personnel action), island ports and critical infrastructure (cargo flow anomaly detection), and island hospitality and tourism (rapid baseline calibration for high-turnover environments).

## V. Policy Recommendations

1. Require island-specific insider threat assessment framework compliance for critical infrastructure operators in Hawaii and Pacific Island territories, replacing continental frameworks these organizations cannot meaningfully implement.
2. Fund shared third-party threat assessment services for small island-state organizations through state, territorial, or federal grants — reducing per-organization cost while maintaining the external independence that makes third-party assessment effective.
3. Commission culturally calibrated behavioral baseline research for Pacific Island and Native Hawaiian organizational environments — research that does not exist in the published literature and is required for accurate BTAM application in these contexts.
4. Reform federal insider threat program compliance requirements for Pacific Island territory governments to recognize the structural constraints of small island agencies and prescribe achievable compensating controls.
5. Establish island-specific insider threat compliance capacity as a criterion in Hawaii and Pacific territory security grant eligibility assessments.

## VI. Conclusion

The insider threat problem in small island-state organizations is not smaller than the insider threat problem in large continental organizations. ISPI's practitioner analysis indicates it may be larger — because the detection infrastructure is weaker, the reporting barriers are higher, and the consequences of an undetected insider incident in a supply-chain-dependent, sole-provider island community can cascade in ways that continental communities with redundant systems are structurally protected from.

ISPI accepts commissions for insider threat assessment framework development, organizational threat assessments, and training program delivery for island and Pacific territory organizations. Contact ISPIGlobal@proton.me or visit ispiglobal.com/commission.

NOTES AND REFERENCES

## ABOUT THE ISLAND SECURITY POLICY INSTITUTE

The Island Security Policy Institute (ISPI) is a nonprofit, nonpartisan research organization based in Honolulu, Hawaii. ISPI produces practitioner-led research, policy analysis, training programs, and commissioned research on public safety, emergency preparedness, insider threat, and security policy for island and coastal communities worldwide. ISPI is registered as a federal contractor on SAM.gov under NAICS 541720. Warren Pulley, Founder & Executive Director.

Website: ispiglobal.com · Email: ISPIGlobal@proton.me · Phone: (808) 999-0544 · LinkedIn: linkedin.com/in/warpul13