ISLAND SECURITY POLICY INSTITUTE

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

POLICY BRIEF

The Insider Threat in Small Organizations

Why Detection Frameworks Built for Large Institutions Fail Island-State Workplaces

---

Research Pillar: Insider Threat & Workplace Security Policy

Document Type: Policy Brief

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 small organizations Hawaii, workplace security island communities, behavioral threat assessment BTAM Hawaii, insider threat detection Pacific Islands

---

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.

© 2026 Island Security Policy Institute · Independent · Nonpartisan · 501(c)(3) · ispiglobal.com

The Insider Threat in Small

Organizations

Why Detection Frameworks Built for Large Institutions Fail Island-State Workplaces — and What to Do About It threat assessment, island workplace security, BTAM Hawaii, threat assessment Pacific, insider threat small business, workplace violence prevention island communities the State of Hawaii. This publication represents ISPI's independent research and policy analysis. The views expressed herein do not necessarily reflect the position of any funder, sponsor, or affiliated organization. ISPI maintains full editorial independence on all research outputs. Full institutional credential documentation is available to qualified government agencies, foundations, and institutional partners upon formal request. In March 2022, a Hawaii county government agency discovered that an employee had been systematically accessing and exfiltrating sensitive infrastructure data for eleven months before anyone noticed. Post-incident review revealed that colleagues had observed concerning behavioral changes — increased secrecy, unusual after-hours access patterns, expressions of financial grievance — but had not reported them. The reasons were not apathy or negligence. The employee was a well-liked colleague of fifteen years whose family was known throughout the community. In a workplace of thirty-two people on a small island, the social cost of making a formal report felt, to those who noticed, prohibitively high. This case is not unusual. ISPI's practitioner analysis of more than 2,400 documented threat assessments across Hawaii, nationally, and internationally identifies a consistent pattern: insider threat incidents in small island-state organizations are systematically preceded by behavioral warning signs that colleagues observed and did not report. The detection failure is not a training failure. It is a framework failure — the application of insider threat detection tools designed for large continental organizations to social environments those tools were never designed to address.

Key Findings

Insider threat detection frameworks developed by the Carnegie Mellon CERT Insider Threat Center, the National Insider Threat Task Force, and the DHS Insider Threat Program assume organizational scale — dedicated security personnel, anonymous reporting mechanisms, and institutional distance between colleagues — that small island-state organizations typically do not have. In island community workplaces where professional and personal networks overlap substantially, the social cost of formal threat reporting is sufficiently high that underreporting of behavioral warning signs is systematic rather than exceptional. ISPI's practitioner analysis indicates this dynamic is the single most important factor distinguishing insider threat outcomes in

© 2026 Island Security Policy Institute · Independent · Nonpartisan · 501(c)(3) · ispiglobal.com

islandstate organizations from large continental organizations. Available research on organizational reporting behavior in small, socially dense environments — including Vaughan's work on normalization of deviance and Edmondson's research on psychological safety — suggests that anonymous reporting mechanisms are largely ineffective in communities where anonymity is structurally impossible. Alternative reporting architecture is required. ISPI's practitioner knowledge base identifies four behavioral indicators that are systematically missed or normalized in small island-state organizational environments, each requiring islandspecific detection calibration rather than standard continental threat indicator thresholds.

The Detection Framework Gap

The foundational assumption of every major insider threat detection framework is organizational scale sufficient to create institutional distance between colleagues. This assumption shapes every element of standard detection architecture: anonymous tip lines assume reporters cannot be identified; dedicated security personnel assume a workforce large enough to sustain non-operational roles; formal HR investigation functions assume case volumes sufficient to develop and maintain investigative expertise. Island-state workplaces — resorts, hospitals, port authorities, small government agencies, schools — typically operate with workforces ranging from 15 to 150 people in communities where everyone, in the relevant social sense, knows everyone. Anonymous tip lines are not anonymous in these environments. Dedicated security personnel are not available. Formal HR investigation functions are not sustainable. The detection architecture that large-organization frameworks prescribe is, in small island-state organizational contexts, largely inoperative. The result is a systematic detection gap that creates risk that is invisible to standard risk assessment tools — because those tools measure detection capacity by the presence or absence of framework components rather than by their functional effectiveness in the specific organizational context.

Four Indicators Systematically Missed in Island Organizations

I. Gradual Access Privilege Escalation

In large organizations, access control logs are routinely audited by dedicated security personnel who identify privilege escalation patterns without social friction. In small island organizations, access control may be managed by an administrator who is also a social peer of the person whose access patterns are changing. Incremental privilege escalation — each individual step seemingly reasonable — is consistently normalized in small organization contexts where access decisions are interpersonal rather than institutional. ISPI's practitioner

© 2026 Island Security Policy Institute · Independent · Nonpartisan · 501(c)(3) · ispiglobal.com

analysis indicates that access privilege escalation is the most reliably detectable indicator in small island organizations precisely because it generates a digital record that can be reviewed without interpersonal friction — if a third-party review mechanism exists. In the absence of such a mechanism, it is systematically missed.

II. Financial Stress in High Cost-of-Living Environments

Hawaii and Pacific Island territories have among the highest costs of living relative to median income in the United States. Financial stress is sufficiently endemic in island communities that it functions poorly as a standalone behavioral indicator — it describes too large a proportion of the workforce to be discriminating. ISPI's practitioner analysis suggests, however, that changes in financial behavior — rather than financial stress per se — retain their indicator value in island contexts and require culturally-calibrated assessment to identify correctly.

III. Social Withdrawal in High-Baseline Connection Environments

Standard insider threat frameworks identify social withdrawal as a behavioral indicator partly because continental organizational baselines assume moderate social connection among colleagues. In close-knit island workplaces where social connection is deep and longstanding, the same behavioral change represents a more significant departure from baseline and carries proportionally greater indicator weight. Island-specific threat assessment must calibrate to community social baseline rather than continental organizational norms.

IV. Grievance Expression in High-Context Cultural Environments

Pacific Island and Native Hawaiian cultural contexts involve communication patterns — including grievance expression — that differ substantially from the mainland cultural norms embedded in standard threat indicator training. Indirect grievance expression, deference-based communication, and culturally-specific conflict avoidance patterns may present to mainlandtrained assessors as absent grievance when substantive grievance is present. ISPI's practitioner knowledge base informs culturally-calibrated behavioral baseline assessment for Pacific Island and Hawaii community organizational environments.

Policy Recommendations

1. Replace anonymous tip lines — which the available evidence suggests are largely ineffective in small island-state organizational environments — with structured third-party assessment pathways that remove social cost from the

© 2026 Island Security Policy Institute · Independent · Nonpartisan · 501(c)(3) · ispiglobal.com

reporting process by placing it outside the organizational social network entirely.

2. Mandate BTAM-certified threat assessment training for security

personnel in critical island-state infrastructure organizations — ports, hospitals, utilities, government agencies — with training curricula adapted for small organization and island community contexts.

3. Commission development of island-specific behavioral baseline

research to calibrate threat indicator thresholds for Pacific Island and Hawaii community organizational environments, distinct from the continental organizational baselines currently embedded in standard detection frameworks.

4. Establish third-party threat assessment referral mechanisms for small

island-state organizations that provide access to professional assessment capacity without requiring the small organization to develop and sustain that capacity internally.

5. Include island-specific insider threat detection framework

requirements in DHS security grant conditions for critical infrastructure operators in Hawaii and Pacific territories.

Conclusion

The insider threat risk in small island-state organizations is not smaller than the risk in large continental organizations. The available evidence suggests 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 island community can cascade in ways that continental communities are structurally protected from. Closing this gap requires not better application of existing frameworks but the development of island-specific frameworks calibrated to the actual organizational and social environments of island communities. ISPI's research program is producing that development. Institutions seeking to commission island-specific insider threat assessment framework development may contact ISPI at ISPIGlobal@proton.me or visit 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's research draws on verified operational experience across U.S. military service, metropolitan law enforcement, diplomatic security operations, FEMA-certified emergency management, and campus safety administration. ISPI is registered as a federal contractor on SAM.gov under NAICS 541720. To commission research, subscribe to ISPI publications, request the ISPI Policy Advisor institutional

© 2026 Island Security Policy Institute · Independent · Nonpartisan · 501(c)(3) · ispiglobal.com

access, or inquire about training programs and speaking engagements: purposes with full attribution to the Island Security Policy Institute. For commercial reproduction or translation rights, contact ISPIGlobal@proton.me.

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

© 2026 Island Security Policy Institute. All rights reserved. This publication may be reproduced for noncommercial purposes with full attribution to ISPI.