Building NITTF-Aligned Insider Risk Programs for Government Organizations

The NITTF guidelines provide government organizations with a clear, authoritative framework for establishing and strengthening insider threat programs. When applied effectively, they help agencies align policy, governance, and operational practices to better detect, deter, and mitigate insider risk.

This checklist translates core NITTF guidelines into a practical, operational framework to help you assess your current program, identify areas for improvement, and reinforce consistent, sustainable alignment across people, processes, and technology.

1. Program leadership and governance

A successful insider risk program starts with clear ownership, accountability, and governance. Leadership alignment ensures risk is addressed consistently, lawfully, and with executive visibility.

Designate a senior official responsible for the insider threat program	☐
Establish a cross-functional governance body (security, HR, IT, legal, privacy)	☐
Define roles, responsibilities, and decision-making authority	☐
Document policies, procedures, and compliance requirements	☐
Align insider risk objectives with agency mission and risk priorities	☐

Ontic provides role-based dashboards and governance workflows that give leadership real-time visibility into insider risk activity, program performance, and accountability across stakeholders.

2. Insider risk program personnel

An effective program relies on skilled and trusted personnel who understand both security risks and legal boundaries. Cross-disciplinary expertise enables balanced, defensible decision-making.

Assign personnel with expertise across physical security, cyber, HR, legal, and behavioral analysis	☐
Ensure personnel receive appropriate insider risk and privacy training	☐
Clearly define investigative authority and escalation thresholds	☐
Establish secure collaboration processes between participating teams	☐

Ontic centralizes case management and workflows, enabling consistent investigations, collaboration across departments, and auditable decision trails.

3. Training and workforce awareness

Training and awareness are critical to early detection. Employees should understand insider risk indicators, reporting expectations, and the program's purpose without fear of retaliation.

Deliver insider risk training within 30 days of onboarding	☐
Conduct annual refresher training for all personnel	☐
Provide role-based and scenario-driven training where applicable	☐
Promote a culture of reporting and shared responsibility	☐
Offer anonymous or confidential reporting mechanisms	☐

Ontic supports training tracking, standardized reporting intake, and documentation that reinforces transparency and accountability across the workforce.

4. Access to relevant information

Timely access to relevant information helps insider risk teams identify concerning patterns while remaining compliant with legal and privacy requirements.

Identify required data sources (HR, IT, physical access, security systems)	☐
Establish lawful data-sharing agreements and access controls	☐
Ensure data is available to authorized personnel when needed	☐
Protect sensitive information through role-based access and audit logs	☐
Offer anonymous or confidential reporting mechanisms	☐

Ontic integrates disparate systems into a single platform, securely centralizing data while enforcing strict access controls and compliance safeguards.

5. Monitoring and detection

Monitoring should move beyond isolated signals to holistic detection that considers behavioral, digital, and physical indicators together.

Monitor user activity across cyber and physical environments	☐
Identify high-risk behaviors over time	☐
Correlate signals across multiple data sources	☐
Shift from reactive investigation to proactive risk identification	☐

Ontic aggregates cyber, physical, and behavior signals into one connected platform, helping teams identify emerging insider risks earlier and with greater context.

6. Integration, analysis, and response

Detection alone is not enough. Agencies must be prepared to analyze indicators, coordinate response, and act quickly and consistently.

Define standard operating procedures for insider threat response	☐
Clarify response roles across security, HR, legal, and leadership	☐
Conduct regular tabletop exercises and program reviews	☐
Ensure investigations are documented, repeatable, and defensible	☐

Ontic centralizes every step — intake, triage, response, resolution, and reporting — into a single platform that adapts to your structure and integrates with the rest of your security operations.

7. Reporting, metrics, and continuous improvement

Ongoing measurement and reporting help you demonstrate compliance, identify gaps, and continuously mature your insider risk program over time.

Track key metrics (training completion, cases, response times)	☐
Provide leadership with regular program reporting	☐
Maintain documentation and records retention policies	☐
Benchmark progress against the NITTF maturity framework	☐
Use insights to refine processes and improve outcomes	☐

Ontic delivers reporting and analytics that support audits, leadership briefings, and long-term program maturity planning.