OPERATIONAL SECURITY FOR TRIBAL COURTS

A Tribal Court Security & Confidentiality Toolkit — National Native Justice Institute | www.nativejustice.us

■ OPERATIONAL SECURITY IN TRIBAL COURT ENVIRONMENTS

Operational Security (OPSEC) is the practice of protecting sensitive information, operational plans, and personnel identities from individuals who could use that information to cause harm. In tribal court settings, OPSEC protects judicial personnel, high-risk witnesses, in-custody defendants, sensitive case information, and the security measures that protect all of them. In small tribal communities, where personal relationships and information networks are extensive, OPSEC requires active, conscious management of what information is shared, with whom, and through what channels.

In close-knit tribal communities, security-relevant information travels rapidly through personal and social networks. Information about judges' routines, scheduled hearings, and security measures must be treated as sensitive operational data.

Social media is the greatest OPSEC threat in modern tribal court security. Court personnel, security officers, and even judges who post work-related information online may inadvertently expose protected persons to harm.

OPSEC is everyone's responsibility — not just the security officer's. Clerks, attorneys, advocates, and administrative staff who handle scheduling, witness information, and case data are all OPSEC stakeholders.

Every OPSEC breach — however inadvertent — should be documented, assessed for harm, and used as a training opportunity to prevent future occurrences.

■ INFORMATION PROTECTION IN TRIBAL COURT OPERATIONS

What Information Requires OPSEC Protection

- Judicial personnel home addresses, personal phone numbers, vehicle descriptions, and daily routines.
- Witness and victim addresses, contact information, protective order details, and safety plans.
- Scheduled hearing dates and times for high-risk cases before they are publicly docketed.
- Security staffing levels, post assignments, equipment locations, and response protocols.
- In-custody defendant transport schedules, arrival times, and holding area configurations.
- Judicial threat intelligence: known threats, individuals of concern, and protective measures in place.

Common OPSEC Vulnerabilities in Tribal Courts

- Discussing case schedules, witness identities, or security measures in public areas of the courthouse where parties to proceedings may overhear.
- Posting courtroom or hearing-related information on social media — including photographs that inadvertently reveal witness identities or courtroom security measures.
- Leaving sensitive documents — docket sheets, victim contact information, or security plans — visible on desks or in common areas accessible to court visitors.
- Using personal phones or unencrypted email for communications containing protected case or personnel information.

■ OPSEC PRACTICES FOR COURT SECURITY PERSONNEL

Personal Security Practices

- **Control Your Digital Footprint** – Security officers should review their own social media accounts and ensure that no posts reveal their employer, work schedule, security equipment, or case-related information.
- **Protect Judicial Personnel Information** – Never confirm a judge's location, schedule, home address, or vehicle to any person who contacts the court without a verified, legitimate need to know.
- **Use Secure Communications for Sensitive Information** – Case-sensitive communications between court security, tribal police, and judicial personnel should occur through secure channels — not personal text messages or public radio frequencies.

Institutional OPSEC Practices

- **Need-to-Know Information Access** – Access to scheduling, witness information, security plans, and judicial personnel data should be restricted to those with a documented operational need.
- **Docket Publication Timing** – For high-risk cases, limit public docket publication to the minimum advance notice required by tribal court rules. Early publication of high-risk hearing schedules creates unnecessary exposure.
- **Secure Document Handling** – Sensitive documents must be stored in locked files when not in active use, shredded when no longer needed, and never left visible in public areas of the courthouse.

RESOURCES, GRANTS & SUPPORT

Funding, Training, and Support Resources — Tribal Court Operational Security Programs | www.nativejustice.us

FEDERAL GRANT RESOURCES

Court Security Funding

- **COPS Tribal Resources Grant (TRG)** – Funds tribal public safety including court security staffing, training, and equipment. cops.usdoj.gov/tribalresources
- **CTAS – Coordinated Tribal Assistance Solicitation** – DOJ consolidated tribal funding for courts, law enforcement, and security programs. justice.gov/tribal
- **BJA Tribal Justice Programs** – Supports tribal court operations and court security capacity. bja.ojp.gov/program/tribal-justice
- **FEMA Tribal Homeland Security Grant Program (THSGP)** – Annual DHS funding for tribal security infrastructure and emergency preparedness. fema.gov/tribal

Information Security & OPSEC

- **DHS CISA – Security Awareness Training** – Federal information security awareness resources applicable to tribal court OPSEC programs. cisa.gov
- **FBI – Counterintelligence & Insider Threat** – Federal resources on information protection and insider threat applicable to tribal court settings. fbi.gov
- **National Center for State Courts – Court Security** – Court security information protection standards and training resources. ncsc.org

STATE & ADDITIONAL RESOURCES

- **State Court Security Standards** – Most state court administrative offices publish court security standards applicable to tribal courts under intergovernmental agreements. Contact your State Court Administrator.
- **State Homeland Security Grants (SHSGP)** – Tribal court security programs may be eligible for state-administered FEMA homeland security funding. Contact your State Administrative Agency (SAA).
- **Tribal Law & Order Act (TLOA) Resources** – TLOA expanded tribal justice authority and DOJ technical assistance for tribal courts and security programs.
- **Grants.gov Tribal Search Tool** – Search all federal grants available to tribal entities. grants.gov (filter: Tribal Government eligibility)

HELPFUL TIPS FOR TRIBAL PROGRAMS & LEADERS

Adopt a Written Court Security Information Policy A formally adopted information policy defining what court security data is protected, who may access it, and what the consequences of unauthorized disclosure are is the foundation of an OPSEC program.	**Implement a Social Media Policy for All Court Personnel** A clear, written social media policy for all court employees — not just security staff — is the most impactful single OPSEC measure available to a tribal court.
Conduct Annual OPSEC Training for All Court Staff Annual OPSEC awareness training covering social media risks, document handling, verbal security, and communication protocols ensures that every court employee understands their role in protecting sensitive information.	**Audit Public Information Sources Annually** Search your tribal court's name, judicial personnel names, and facility address annually to identify what information is publicly accessible and whether any of it creates unnecessary security exposure.

KEY WEBLINKS

National Native Justice Institute	*www.nativejustice.us*
National Center for State Courts	*ncsc.org*
COPS Tribal Resources Grant	*cops.usdoj.gov/tribalresources*
BJA Tribal Justice Programs	*bja.ojp.gov/program/tribal-justice*
DHS CISA Security Awareness	*cisa.gov*
FBI Counterintelligence	*fbi.gov*

PARTNER WITH NNJI — WE ARE READY TO SUPPORT YOUR COMMUNITY

TAKE ACTION TODAY — Contact NNJI at **www.nativejustice.us** to schedule training, consultation, or access resources.

Strengthening Tribal Justice — One Community at a Time