

Comprehensive Transition Plan from a legacy PSAP utilizing e911 to a Next Gen PSAP utilizing NG911



Phase 1: Planning and Comprehensive Assessment

Initial Needs Assessment and Gap Analysis

Conduct a thorough assessment of your current legacy PSAP environment, covering technology, staffing, and security. Identify outdated infrastructure, bandwidth limitations, and gaps in multimedia support. Evaluate staff competencies against NG911 requirements. Determine where you stand regarding CJIS compliance to handle Criminal Justice Information (CJI).

Stakeholder Engagement and Governance Establishment

Form a governance committee that includes local, state, and federal partners, 911 boards, IT directors, law enforcement, and legal advisors. Ensure multi-agency coordination to align on standards, interoperability, and funding objectives.

Funding and Budgeting Strategy

Identify and secure funding streams, including federal grants (DHS, CISA, FEMA), state funds, and local appropriations. Develop a multiyear financial roadmap that aligns with procurement and deployment phases.

Legal and Regulatory Review

Review state-specific 911 statutes, federal mandates (such as FCC requirements), and data retention obligations. Ensure planned changes comply with wiretap laws, public records access, and criminal procedure requirements.

CJIS Compliance Baseline Assessment

Conduct a CJIS Security Policy gap analysis. Examine data encryption (at rest and in transit), access controls, audit logging, multi factor authentication (MFA), and physical security measures. Document deficiencies and prioritize fixes, since NG911 will likely process more CJI.

Geographic Information System (GIS) Data Preparation and Validation

Update centerline files, address point layers, and PSAP boundary datasets. Accurate GIS data is essential for NG911 call routing to the correct PSAP.

Phase 2: Infrastructure and Technology Upgrade with Security as a Foundation

Establishing an Emergency Services IP Network (ESInet)

Design and procure a secure, resilient IP-based ESInet. Ensure the network has redundancy, failover capabilities, and bandwidth to support voice, text, video, and data.

Implementing a CJIS Compliant Network Architecture

Adopt network segmentation, deploy intrusion detection and prevention systems (IDS/IPS), and implement next-generation firewalls. Ensure all network elements handling CJI meet CJIS encryption and logging requirements.

Adopting Zero Trust Network Access (ZTNA)

Implement a Zero Trust security model where access is granted only after verifying user identity, device security posture, and access context. Replace perimeter-based trust with continuous authentication and authorization, applying principles such as least privilege and microsegmentation.

Upgrading PSAP Equipment and Software

Replace legacy call handling equipment with IP-based systems (VoIP CHE), integrate Next Generation CAD, and update recording systems to support multimedia. Ensure new systems are CJIS capable and support encryption aligned with NIST standards.

Multimedia and Text-to-911 Capabilities Integration

Deploy solutions that enable the receipt and processing of text, image, and video communications. This is critical for meeting public expectations and improving situational awareness.

Security and Resilience Planning

Develop a cybersecurity strategy aligned with CJIS. Include incident response, disaster recovery, business continuity, data backup, and data integrity verification. Leverage recommendations from NIST and DHS to harden systems against evolving threats.

Cloud Service Provider (CSP) Vetting

If you plan to use cloud services (for CAD, mapping, or data storage), ensure the provider is CJIS compliant and willing to sign the FBI's CJIS Security Addendum. Evaluate the provider's audit trails, encryption capabilities, and incident response readiness.

Phase 3: Rigorous Testing, Training, and Public Engagement

System Integration Testing

Conduct comprehensive end to end tests of the ESInet, CHE, CAD, logging, and mapping systems. Validate call flow, location accuracy, and multimedia handling.

Operational Readiness Testing

Simulate real world emergency scenarios to ensure systems function correctly under load. Validate failover operations and disaster recovery.

Comprehensive Staff Training (Technical and Security Awareness)

Train call takers, dispatchers, IT staff, and administrators on new workflows and NG911 technologies. Provide specialized training on CJIS Security Policy requirements, data handling, phishing awareness, and use of ZTNA systems.

Public Education and Outreach

Inform the community about new services such as Text to 911. Use social media, local media, and community meetings to explain how NG911 improves emergency response.

Security Audits and Compliance Verification

Perform internal audits and contract external assessments to verify CJIS compliance before going live. Address non-compliant findings immediately.

Phase 4: Go-Live, Optimization, and Continuous Compliance

Phased Rollout Strategy

Gradually transition call traffic to NG911 systems by jurisdiction or call type to minimize disruption. Monitor performance closely.

Legacy System Decommissioning

Securely retire legacy E911 systems. Ensure all data is sanitized according to CJIS and NIST guidelines to prevent unauthorized access.

Continuous Monitoring and Optimization

Implement 24/7 security monitoring using SIEM systems and integrate threat intelligence feeds. Tune system performance and security policies regularly.

Ongoing Maintenance and Support

Establish vendor maintenance agreements and build internal IT capabilities for rapid troubleshooting and system updates.

Regular CJIS Compliance Reviews and Updates

Schedule periodic internal audits and external reviews. Refresh staff training annually or when major CJIS updates occur. Regularly evaluate and adjust ZTNA policies and logs to maintain robust security postures.

Why This Plan Matters

Transitioning to NG911 is not just a technological upgrade but a mission-critical move to enhance public safety, support modern emergency communications, and protect sensitive data. The integration of Zero Trust Network Access and adherence to CJIS compliance ensures your agency remains resilient against evolving cybersecurity threats, including future quantum computing risks.

Suggested Next Steps

Use this framework to build a detailed NG911 transition project plan tailored to your agency. Engage with your state's 911 coordinating authority and federal grant programs for funding opportunities. Begin vendor consultations to assess CJIS compliant and Zero Trust capable solutions. Reach out to 911nurd for consultation or visit

<https://www.911nurd.com> for more information.

911 Phone System (CHE & ESInet) Transition Checklist

- Complete technical gap analysis focused on current call handling equipment (CHE), legacy trunks, and NG911 readiness.
- Form governance committee with telecom, GIS, and local/state 911 coordinators.
- Secure funding for NG911 phone infrastructure (grants, state/local funds).
- Conduct full legal/regulatory review to ensure state 911 compliance.
- Complete CJIS compliance baseline audit of CHE systems, logging, and call recordings.
- Validate and update GIS data layers (centerlines, address points, PSAP boundaries) for NG911 routing.
- Design and procure secure, redundant ESInet with guaranteed SLAs.
- Implement network segmentation, IDS/IPS, and CJIS compliant encryption across the ESInet and CHE environment.
- Deploy Zero Trust Network Access (ZTNA) for CHE user and device authentication, with MFA and endpoint validation.
- Upgrade CHE to support VoIP, SIP call delivery, and multimedia.
- Enable text-to-911, photo, and video call support with secure handling of multimedia data.
- Draft and test CHE-focused cybersecurity incident response and continuity plans.
- Vet Cloud Service Providers (if CHE or call logging is cloud-based) for CJIS compliance and secure contracts.
- Perform CHE system integration and end-to-end operational readiness tests.
- Train call takers and telecom staff on NG911 workflows, secure multimedia handling, and CJIS data rules.
- Educate the public about Text to 911 and new NG911 capabilities.
- Perform security audits specific to CHE and ESInet for CJIS compliance.
- Roll out NG911 phone services in planned phases (e.g., by trunk group or region).
- Securely decommission legacy E911 call systems and sanitize stored data.
- Implement 24/7 monitoring, threat intelligence feeds, and alerting on CHE systems.
- Schedule ongoing CJIS compliance reviews and refresher training.

CAD System Transition Checklist

- Complete technical and compliance gap analysis focused on CAD software, databases, and data sharing.
- Include CAD vendor representatives in governance committee to align on interfaces and compliance.
- Secure funding for CAD upgrades (consider CAD-specific grants or regional sharing initiatives).
- Review state regulations on CAD data retention, incident records, and CJIS requirements.
- Complete CJIS baseline audit for CAD system access controls, logs, and encryption at rest.
- Implement network segmentation, IDS/IPS, and robust encryption on CAD infrastructure.
- Deploy Zero Trust controls on CAD systems with MFA, device posture checks, and least privilege roles.
- Upgrade CAD software to NG911-compatible versions that can receive location-rich data and multimedia from CHE.
- Integrate GIS datasets into CAD for improved situational awareness and mapping precision.
- Develop and test CAD-specific incident response and disaster recovery plans.
- If using CAD SaaS/cloud services, vet providers for CJIS compliance and sign FBI security addendums.
- Conduct integration testing of CAD with CHE and radio systems (end-to-end dispatch flow).
- Train dispatchers and supervisors on new CAD features, CJIS data security, and Zero Trust practices.
- Perform internal/external audits to validate CAD environment CJIS compliance.
- Schedule phased CAD cutovers to minimize operational impact.
- Decommission legacy CAD databases securely with documented data sanitization.
- Establish continuous monitoring of CAD logs, access, and performance.
- Include CAD in regular CJIS policy reviews and security training updates.

Radio System Transition Checklist

- Conduct gap analysis of current radio console integrations, logging recorders, and encryption standards.
- Include radio vendors and local/state radio interoperability coordinators in the governance discussions.
- Secure funding specifically for console upgrades and new radio network integrations with NG911.
- Review state/federal interoperability standards (e.g., P25, ISSI) and retention requirements for radio transmissions.
- Complete CJIS audit focusing on radio console systems, voice logging, and access to CJI via radio.
- Segment the radio network from other IT systems with strict firewalls, deploy IDS/IPS, and enforce encryption of console traffic.
- Implement Zero Trust controls on radio console access with user verification and MFA.
- Upgrade radio consoles and logging equipment to ensure compatibility with NG911-provided incident metadata.
- Develop a radio-focused incident response and failover plan (e.g., fallback to conventional channels).
- If using cloud-based logging or console control, ensure CJIS compliance and signed addendums with the provider.
- Test interoperability between upgraded radio consoles, new CAD systems, and multimedia CHE feeds.
- Train radio operators on new console workflows, encryption requirements, and Zero Trust protocols.
- Perform radio system security audits tied to CJIS policy.
- Plan phased radio console and logging system cutovers to maintain continuity.
- Securely retire old radio consoles and sanitize recorded audio data.
- Implement radio console and network monitoring for anomalies and unauthorized access.
- Include radio systems in ongoing CJIS compliance reviews and staff security training refreshers.

Detailed CJIS Compliance Tracking Sheet

Use this table to monitor and document CJIS compliance efforts across key requirements.

CJIS Security Requirement	Current Status / Notes	Responsible Party
Encryption at rest and in transit meets CJIS standards		
Multi Factor Authentication implemented for CJI access		
Audit logging configured and logs reviewed regularly		
Access control policies enforced (least privilege, role based)		
Physical security controls (facility access, cameras, locks) in place		
Intrusion detection and prevention systems operational		
Security incident response plan documented and tested		
CSP agreements signed with CJIS Security Addendum		
ZTNA policies applied to all CJI access		
Regular staff training on CJIS requirements completed		
Routine internal and external CJIS audits performed		

Document published July 2025.

About the Authors

Brian Nelson

Brian Nelson is the president of 911nurd, bringing more than 25 years of hands-on experience in public safety technology. His background includes decades managing, maintaining, and evolving critical 911 infrastructure, from CAD systems and telephony to radio networks and multi-agency operational platforms.

Brian partners directly with PSAPs, emergency management teams, and first responder leadership to modernize 911 environments, plan and execute complex system transitions, and ensure mission-critical resilience under demanding conditions. Known for his vendor-neutral perspective and practical problem-solving, he bridges technical design with the operational realities of public safety, helping agencies navigate next-generation network deployments, cybersecurity initiatives, and large-scale technology consolidations.

Earlier in his career, Brian served as a 911 Systems Administrator and project leader in Rock Island County, Illinois, where he oversaw system performance, compliance, and modernization for more than two decades. His experience is also grounded in military service as an aviation operations specialist and information systems analyst in the U.S. Army, adding a disciplined, mission-focused perspective to his work.

Kenyon Langford

Kenyon Langford is the COO of 911nurd, where he leads strategic planning, financial stewardship, and operational oversight for technology initiatives serving the public safety sector. Drawing on more than two decades of executive leadership in IT, healthcare, and critical communications, Kenyon guides agencies through complex technology modernization projects and helps ensure secure, compliant deployments tailored to the unique demands of emergency services.

His experience spans roles as CIO and Vice President in healthcare and private sector technology environments, coupled with a deep focus on aligning business strategy with operational excellence. At 911nurd, Kenyon brings this background to the development and implementation of secure, next-generation public safety networks, fostering trusted partnerships and cultivating strong teams that support agencies' evolving needs.