Atascosa County Cybersecurity and Infrastructure Resilience Initiative

Proposal Narrative Attachment

1. Description of the Issue

Atascosa County currently operates a highly decentralized and aging technology environment that creates operational and cybersecurity risk for law enforcement, court operations, juvenile justice functions, and related County services. The County supports approximately 1,500 devices across 28 buildings and 40 departments. Each location generally maintains its own internet connection and local network, resulting in a fragmented environment with inconsistent controls, limited centralized visibility, and uneven resilience. For criminal justice purposes, this environment directly affects the Sheriff's Office, Justice Center, Courthouse, four Justice of the Peace precincts, the Juvenile Justice Center, and the Old Jail facility that houses the Fire Marshal, Emergency Management, and the Emergency Operations Center. Shared County systems and interconnected facilities also create a risk pathway into criminal justice systems if the wider environment remains weak.

A substantial portion of the County's network infrastructure is beyond end-of-service life. Approximately ninety percent of switches and wireless access points are legacy or consumer-grade devices that do not provide the visibility, policy control, or reliability needed for secure justice operations. Most switching is unmanaged and therefore does not support modern segmentation, centralized monitoring, or efficient troubleshooting. Wireless infrastructure is similarly inconsistent and, in many cases, unsuitable for a modern public-sector environment that must protect sensitive data while supporting mobile users and distributed facilities.

The County's perimeter security is also inconsistent. Although SonicWall firewalls are already deployed at certain locations, many facilities still depend on consumer-grade or provider-supplied routing equipment, and existing firewall assets are not yet fully standardized under a centrally managed architecture. Network segmentation exists only at a limited interface level where CJIS needs have demanded it. Outside those limited enclaves, the County remains vulnerable to lateral

movement if a workstation, user account, wireless segment, or unmanaged site is compromised. The County has endpoint protection and a SIEM platform in place, but those tools are not currently configured to deliver the real-time alerting, coordinated response, and governance structure needed to operate as a mature program.

The County has already experienced the practical consequences of this environment. Internet outages and infrastructure instability disrupt operations and force staff into a reactive posture. Legacy practices such as adding connections with small unmanaged hubs continue to create fragility and limit visibility. Phishing and malware activity are persistent concerns. Most importantly, recent lightning strikes have demonstrated how narrow the County's margin for error has become. A strike over the weekend damaged an interface at the Justice of the Peace Precinct 2 location. The County was fortunate that the incident did not destroy the entire firewall, because a full failure would have caused a major interruption to court operations at that site. Similar single points of failure exist at many facilities because redundant internet connectivity and power protection are not consistently in place.

This problem is not merely technical. It affects the County's ability to administer the criminal justice system effectively and securely. Sheriff's Office personnel, courts, juvenile detention, and emergency management functions all depend on stable connectivity and secure access to systems and records. If criminal justice systems are unavailable, poorly segmented, or insufficiently monitored, the County risks delayed service, loss of investigative or court productivity, disruption of hearings and case processing, and exposure of criminal justice information. The wider County environment also holds other sensitive data, including health, personnel, and financial information, and weaknesses in those areas increase the chance that a compromise elsewhere in the network could spread into criminal justice operations.

The County is also under compliance pressure. It has recently undergone multiple CJIS audits and is awaiting corrective action plans. County leadership is working in good faith to move toward

compliance within realistic budget constraints, but the underlying infrastructure must improve for those efforts to become durable. The County needs the ability to enforce consistent security controls, maintain reliable documentation and governance processes, and reduce its dependence on ad hoc troubleshooting. Without targeted investment, the County will continue operating critical justice infrastructure with known gaps in perimeter security, internal segmentation, monitoring, resilience, and incident readiness.

JAG funds are therefore needed to address gaps in technology improvement resources that directly affect law enforcement programs, court programs, corrections and community corrections functions, and planning/evaluation/technology improvement activities. The proposed project will replace unsupported infrastructure, standardize and centralize key security controls, improve continuity at mission-critical sites, and build the managed cybersecurity capability the County does not currently possess in-house.

2. Project Design and Implementation

Atascosa County proposes the Atascosa County Cybersecurity and Infrastructure Resilience Initiative, a phased technology improvement project designed to strengthen criminal justice operations through better security, visibility, and continuity. The project will be implemented as a unified architecture rather than a collection of isolated purchases. JAG funds will support three coordinated program components: perimeter security modernization, managed network and infrastructure resilience improvements, and managed cybersecurity services.

First, the County will modernize and standardize perimeter security. Rather than discarding every existing firewall investment, the County will use a hybrid lifecycle strategy that retains enterprise-grade firewall assets where appropriate and transitions them into a managed, centrally governed security architecture. Additional managed firewall services and hardware will be deployed where existing protection is inadequate or where consumer-grade equipment remains in use. This approach is cost-conscious and operationally sound. It improves security coverage across all

County locations while focusing first on the sites whose failure would have the greatest impact on criminal justice operations, including the Sheriff's Office, Justice Center, Courthouse, Justice of the Peace precincts, Juvenile Justice Center, and the Old Jail / Emergency Operations Center facility.

Second, the County will replace unsupported switching and wireless equipment with a standardized managed network platform. This component includes new managed switches, Wi-Fi access points, optical modules for uplinks where needed, and a centralized management platform. These upgrades will give County IT the real-time visibility it currently lacks, provide the technical foundation for expanded segmentation, and reduce troubleshooting time when outages or performance issues occur. The County's broader security posture depends on this visibility. A modern firewall architecture cannot be fully effective if the internal network remains opaque and unmanaged. Likewise, managed security services cannot identify and help contain problems if the underlying network cannot report health, changes, and device status.

Third, the project includes resilience improvements needed to make the network upgrade work in the real world. Structured cabling, patch panel cleanup, and network organization are included because the County's legacy cabling environment is inconsistent and, in many places, not ready to support a clean rollout of modern managed infrastructure. This is not cosmetic work. Properly organized cabling reduces troubleshooting time, improves reliability, and supports the consistent deployment of segmented and monitored networks. The project also includes uninterruptible power supplies at key facilities to reduce damage from electrical disturbances and maintain continuity during short outages. This element is directly responsive to the County's recent experience with lightning-related equipment damage and to the operational reality that justice functions cannot remain dependent on unprotected single points of failure.

The project also includes managed cybersecurity services through a Security Team as a Service model. Atascosa County does not currently have the internal staffing depth to operate a mature

cybersecurity program across a distributed environment. Managed services will therefore provide strategic and operational support during implementation and stabilization. The selected service model includes a virtual Chief Information Security Officer; governance, risk, and compliance support; policy lifecycle management; risk assessment and remediation tracking; incident response planning; security engineering guidance; and cybersecurity program management through a centralized portal. These services are not a substitute for County IT operations. Instead, they provide the specialized capability needed to configure and govern the County's security tools, align the program to CJIS and other recognized frameworks, and move the County from reactive troubleshooting to managed risk reduction.

Stakeholder engagement for this project has been practical and operationally driven. County IT has coordinated with the County Auditor during grant planning, and project priorities have been informed by direct awareness of mission-critical sites and the impact of outages and weak controls on justice-related operations. The County's IT leadership is also coordinating the project around current audit and compliance efforts. The County expects ongoing coordination among IT, County leadership, the Auditor's office, justice stakeholders, and implementation vendors as work proceeds. This allows the County to align deployment order with operational risk, rather than using a purely convenience-based rollout.

JAG funds will be coordinated with local County resources in a targeted and responsible way. The County's local funds remain insufficient to execute a countywide modernization effort of this scale in the near term, but County personnel will provide implementation oversight, access coordination, and day-to-day operational support. If minor local costs arise outside the quoted scope, the County can handle them without changing the core project. The County also expects to sustain recurring operational costs after the initial federally supported implementation period, particularly for managed cybersecurity services. This is intentional. The grant-funded period is being used to

establish the program, implement the controls, and stabilize operations so that the County is in a stronger position to sustain the capability.

Over the four-year grant period, the County will use the funds to execute the following program design. In Year 1, the County will prioritize managed firewall deployment, transition retained firewall assets into the managed model, begin network platform rollout, implement structured cabling and UPS improvements at key locations, and start the onboarding and first year of managed cybersecurity services. In Year 2, the County will complete remaining network modernization work, continue managed cybersecurity services, deepen segmentation and policy enforcement, and use the managed service team to formalize governance, documentation, and remediation tracking. In Years 3 and 4, the County will use the stabilized architecture and governance processes created during the implementation period to sustain operations, track performance, and maintain readiness under the award's reporting and compliance expectations. The County does not propose subawards as part of this application.

The expected result is a unified countywide security and resilience architecture that directly strengthens the administration of the criminal justice system. Law enforcement and court sites will be less likely to suffer prolonged outages. The County will be able to identify problems earlier, isolate affected segments more effectively, and respond with more discipline when events occur. The project also supports future improvements that matter to the public, because a County that is no longer consumed by preventable outages and unmanaged security risk can devote more time to improving service delivery.

3. Capabilities and Competencies

Atascosa County has the administrative and technical capacity to implement this project successfully and to meet the associated reporting obligations. The County's IT leadership has already performed substantial planning work for this initiative, including development of a department-based naming scheme, ongoing asset cataloging, evaluation of firewall, switching, and

wireless options, and active CJIS compliance preparation. The County has a realistic understanding of its current limitations and has intentionally chosen a project design that closes those gaps without overextending its internal staff.

From a technical perspective, the County is well positioned to oversee deployment because the proposed design matches its operating reality. The firewall strategy uses a hybrid model that preserves appropriate existing investments while standardizing management. The network strategy standardizes hardware and management under one platform rather than introducing multiple overlapping systems. The managed cybersecurity services component brings in expertise the County does not currently have in-house, especially in governance, risk and compliance, security engineering, policy development, and program oversight. This combination is more credible than attempting to force a small County IT team to build a mature cybersecurity function alone.

From an administrative perspective, the County Auditor is already engaged in the grant planning process, and the County understands that financial controls, procurement discipline, and post-award reporting are essential. The proposal is structured to use direct, traceable costs supported by vendor quotes and service documentation. The County can track implementation through vendor invoices, configuration milestones, inventory records, and managed service reporting. Financial reporting responsibilities will remain with the County's established fiscal management structure, while project management and technical coordination will be led by County IT. This separation of roles supports accountability.

The County will collect and report performance data through a combination of internal records and vendor-supported reporting. Project implementation metrics will include the number of sites moved onto centrally managed perimeter security, the number of managed switches and wireless access points deployed, the number of key locations receiving UPS protection, and the completion of structured cabling cleanup at funded sites. Operational outcome measures will include reductions in preventable downtime at critical justice facilities, increased network visibility across

sites, implementation of segmentation at priority locations, and progress on addressing audit-related control gaps. The managed cybersecurity services platform and recurring reporting process will help the County document risk remediation progress, policy development, and security program milestones. These records will support required performance reporting in the OJP Performance Measurement Tool and in JustGrants.

The County also has evidence-informed reasons for pursuing this strategy. Counties with distributed facilities and limited in-house cybersecurity staffing benefit most when they first improve visibility, standardize the perimeter, reduce obvious single points of failure, and pair technical controls with structured governance. Atascosa County's own experience supports that conclusion. The current environment is hardest to manage where unsupported equipment, unmanaged internal networks, and limited visibility come together. This project addresses those root causes rather than merely reacting to symptoms. It also builds a sustainable path forward by using managed services to establish policy, governance, and risk management processes that can continue beyond the initial implementation period.

Finally, the County participates in broader coordination efforts that inform this project. CJIS remediation work, ongoing audit preparation, vendor coordination, and County leadership discussions about infrastructure modernization have all shaped the final scope. These efforts give the County a grounded understanding of where the most serious operational and compliance risks exist. The proposed project is therefore not speculative. It is the product of direct experience, actual incidents, active compliance efforts, and a practical deployment strategy designed for a small County environment with distributed facilities and limited margin for failure.