Regional Emergency Services and Communications
COMMUNICATIONS & TECHNOLOGY DIVISION - E911
115 S. Andrews Ave, #325 | Fort Lauderdale, FL 33301

MEMORANDUM

DATE: October 8, 2025

TO: Latoya Clark-Forbes, CPPB, NIGP-CPP - Purchasing Assistant Manager

Purchasing Division

FROM: Christopher Oei, Information Technology Specialist - Cyber Security

SUBJECT: Request for Proposals (RFP) No. GEN2129113P1 NextGen 911 – Vendor Security Questionnaire Responses

---

This memorandum provides a summary of the review of the Vendor Security Questionnaires (VSQs) for each of the respondents of the above-mentioned solicitation. The VSQ's purpose is to assess each respondent's security policies and/or system protocols and to identify any security vulnerabilities. Additional questions for clarification were submitted to and responded to by the vendors.

This review is intended to disclose to the Evaluation Committee whether the respondent submitted the VSQ as specified in the solicitation and to make the committee members aware of any apparent security issues. This review is not intended to express an opinion on the respondents' responses.

There were three (3) respondents to the solicitation. All respondents submitted the VSQ, and staff reviewed the same. The following comments are brought to the attention of the Evaluation Committee:

Vendor Name	Comments
ATT	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / External Parties** **Questions 23**: Will third parties, such as IT service providers have access to the County's data that is stored or transmitted by your organization? **Vendor Response**: Yes, Limited to AT&T subcontractor Intrado. **E911 Response:** E911 requires that any privacy / data sharing agreements must ensure that the client data is secure, the vendor should have that language with all 3rd party IT service providers. **AT&T Clarifying Response:** AT&T requires that suppliers contractually adhere to AT&T Supplier Information Security Requirements (SISR). These requirements apply when suppliers:

	• Handle or access AT&T's confidential or proprietary data, including customer information. • Access AT&T's Information Resources, such as systems, networks, or applications. • Provide or support AT&T-branded services using non-AT&T technologies (e.g., cloud services, APIs, mobile platforms). • Develop or customize software for AT&T. • Host or develop websites for AT&T. AT&T Chief Security Office (CSO) has verified that Intrado complies with AT&T's SISR policy. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
ATT	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / External Parties** **Questions 26**: Will third parties, such as IT service providers have access to the County's data that is stored or transmitted by your organization? **Vendor Response**: Yes, Intrado may use offshore resources in Canada and Mexico **E911 Response:** E911 requires information on these external parties: What is their relationship with Intrado? What agreements are in place to protect customer data? **AT&T Clarifying Response:** AT&T's partnership with Intrado is a cornerstone of AT&T ESInet™, combining AT&T's robust network capabilities with Intrado's expertise in 9-1-1 technology solutions. Intrado provides critical technology components within the AT&T ESInet™ core infrastructure. In addition, Intrado assists AT&T with certain aspects of implementation and lifecycle management. Remote access to the network is permitted providing those authorized users are authenticated, and privileges are restricted. Once remote access is granted, it requires a secure VPN client, via equipment which uses an approved firewall, anti-virus protection, up-to-date patching levels, and strong authentication using two factors for authentication. Any connections over the Internet employ a VPN client. Remote access to perform systems administration tasks is achieved over Secure Shell (SSH). AT&T provides Tier 1 technical support to our 9-1-1 customers, including those utilizing AT&T ESInet, through access to the AT&T Resolution Center. The AT&T Resolution Center NOCs are U.S. based and located in Chicago, IL and Atlanta, GA. With regard to how AT&T protects customer data, AT&T requires that suppliers contractually adhere to AT&T Supplier Information Security Requirements (SISR). These requirements apply when suppliers: • Handle or access AT&T's confidential or proprietary data, including customer information. • Access AT&T's Information Resources, such as systems, networks, or applications. • Provide or support AT&T-branded services using non-AT&T technologies (e.g., cloud services, APIs, mobile platforms). • Develop or customize software for AT&T. • Host or develop websites for AT&T.

	AT&T Chief Security Office (CSO) has verified that Intrado complies with AT&T's SISR policy. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
ATT	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Regulatory Compliance** **Questions 35**: Does your organization have a documented process to identify new laws and regulations with IT security implications (e.g., FIPA, new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)? **Question 36:** Yes, Has your organization experienced a data breach within the past five years that legally required reporting under applicable law? **Vendor Response**: Yes **E911 Response:** Is your organization familiar with FLHB7055 and the FLDS reporting requirements? **AT&T Clarifying Response:** AT&T is familiar with FLHB7055 and the FLDS reporting requirements. AT&T will adhere to those State requirements should any data breach containing personal information occur. In addition, AT&T's Chief Information Security Office, External Affairs and Regulatory teams monitor changes in laws and regulations as they pertain to AT&T products and services. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
ATT	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Network Defense and Host Intrusion Prevention Systems** **Questions 86**: Does your organization have any Intrusion Protection System (IPS) in place for your environment? **Vendor Response**: Yes **E911 Response:** E911 requires the additional information on the vendor's IPS solution. Will the vendor support future integration to the County E911 SIEM? **AT&T Clarifying Response:** AT&T's cyber security policies, standards, and guidelines are compliant with industry best practices as defined by International Organization for Standardization and Control Objectives for Information and related Technology. The AT&T ESInet™ infrastructure is built to withstand sophisticated attacks. AT&T ESInet™ is a secured and private IP managed network. All inbound and outbound traffic interactions are with pre-vetted entities, utilize well defined protocols and traverses-controlled access points. Call processing and real-time data delivery are implemented through specialized subnets. AT&T employs a defense-in-depth security strategy where multiple levels of security are in place to provide security and protect sensitive information. Such controls include but are not limited to stateful packet inspection firewalls (host and network based), intrusion detection systems

	(IDS) / intrusion prevention systems (IPS), ACLs, Role-based Access control, multi-factor authentication, strong encryption, and anti-virus and anti-malware including email and host. Furthermore, systems are protected with build standards, patch management, and regular vulnerability scans. Each core emergency call processing site includes border control and security functions including firewalls, intrusion detection systems, and intrusion protection systems. Security management personnel specialize in managing and operating these facilities and validate their operation. The network is capable of processing all traffic, but administratively denies protocols identified as a threat, or that otherwise fall outside of pre-defined IPS parameters. This is partially managed via routing tables and/or Access Control Lists (ACLs). Traffic between core processing sites and distributed sites (e.g., ingress call traffic, PSAPs, management capabilities) is route- and protocol-secure. A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers and firewalls secure the various communication elements of the proposed solution. The network management and service management systems are hardened, require authentication and authorization control, and are instrumented with intrusion detection to assure that they are not compromised and cannot serve as a vector to attack the network or customers. Each core site includes border control functions and security functions including firewalls, and intrusion protection systems. Security management personnel specialize in managing and operating these facilities and validate their operation. Our solution provides for the centralized management of user permissions, rights, and security settings by designated administrators. The system administrators can use the application to manage user roles and privileges, including granular authentication, user profiles, and other security rights to ensure users only have access to applications or data appropriate for them. For any external access, multi-factor authentication and role-based access control are used to restrict user access to the externally facing systems. User access via the public Internet requires two-factor authentication, where one factor is provided through username and password and the second factor is provided through a dynamic, randomly changing secure access code from a provided security token. Users are configured in an identity management system, linked to a specific security token, and configured for access to a defined list of applications and data. Requests for new user accounts or modifications to existing authorized user accounts are tracked and approved through a ticketing system. For internal users, approval is granted through the resource manager and system owner. For external users, confirmation is performed through the applicable AT&T customer engagement representatives prior to account provisioning. A secure identity management portal allows provisioned users to securely enroll contact information and security questions to be used for authenticating a user's identity. For the AT&T solution, we have implemented a defense-in-depth information security methodology, with IPS configuration in place to control and monitor network interfaces and traffic and limit connectivity to known, trusted sources. Implementation of security infrastructure including firewalls, IDS, anti-virus/malware agents, and centralized event logging allow for granular visibility and control across the network. Internal vulnerability monitoring has been implemented across our network, conducting scans on monthly basis, on-demand, or when major changes have been made to infrastructure elements. In addition to internal vulnerability monitoring, we complete annual penetration testing using a third-party

	security vendor to identify potential exposures and vulnerabilities present on AT&T systems. Due to the nature of our network and high availability requirements, testing that could potentially cause system instability or network disruption is performed in a controlled manner to limit the potential impacts to our products and services. The testing methodology used consists of multiple phases including mapping and identifying active devices on the network, scanning devices for vulnerabilities, and attempting to exploit vulnerabilities. Vulnerabilities discovered during penetration testing are mitigated and remediation testing is planned with the penetration testing vendor to validate the mitigation steps that have been implemented. The AT&T ESInet solution is a fully managed solution with a clear demarc defined – so integration with the County's SIEM system is not typically required. AT&T actively monitors all cybersecurity threats and will alert Broward County when/if those threats impact the County's service. Understanding that, the ability exists to share additional logs and events from the AT&T ESInet infrastructure with Broward County, AT&T is open to the idea of creating a solution that best fits Broward's needs. We look forward to jointly designing a solution and monitoring process in partnership with Broward once the future deployment of the County's SIEM solution is designed and requirements are created. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
ATT	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Crypto Materials and Key Management** **Questions 125**: Does your organization have a centralized key management program in place (e.g., any Public Key Infrastructure (PKI), Hardware Security Module (HSM)-based or not, etc.) to issue certificates needed for products and cloud service infrastructure? **Vendor Response**: Yes, AT&T ESInet uses a centralized key management program in place to issue digital certificates to PSAPs to secure transactions. We use proven operational procedures which define creation and maintenance activities such as certificate expiration. AT&T ESInet will be implementing the NIOC's PCA to provide certificates once available. **E911 Response:** E911 requires documentation on your PKI / CA infrastructure and how you handle certificate generation, renewal and revocation. **AT&T Clarifying Response:** Interactions with external ECRFs or the PSAP CPE will utilize digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA). AT&T has been working with NIOC to participate as one of its first subscribers to the NIOC Forest Guide as well as supporting the use of PCA. AT&T has been discussing with Eonti and DigiCert for how to begin the process as a Tier-2 Hosted or Discrete Intermediate Certification Authority (ICA). At this time, Eonti has stated that the process to begin certification as an ICA is pending process finalization but is expected to be completed soon to accommodate our request. Once that moves forward, AT&T will begin providing PCA certificates through the process with DigiCert and Eonti as required by NENA i3 standards. While it is expected that using PCA certificates will begin soon and be operational for i3 PSAPs at the time of delivery, AT&T will continue to manage credentialing

	and issue digital certificates to help ensure protection and security. This mechanism will also be utilized for PSAP access to systems within the AT&T ESInet, including access to the LIS interface, ADR interface and ECRF. At no time will ECRFs used for call routing or PSAP determination provide un-credentialed access. This is due to the potential for Denial of Service (DoS) attacks impacting their critical functions. Following are devices and/or protocols used to restrict access. • AT&T ESInet uses a security border API gateway for i3 data traffic. This device controls access to its services by using client trusted certificates. • Session Border Controllers (SBC) are used for all SIP and SIP related communications. AT&T verifies credentialed devices or that carriers are authorized access in the following manner: o PCA or if unavailable, Client certificates, issued by a trusted Certificate Authority (CA), are required in order to access i3 services such as LIS, ADR, and ECRF. • The trusted CA role is currently provided by AT&T, the role will be filled by them or an authorized NENA PCA vendor once their processes are completed and certification for Hosted ICA can begin for approval. Once the digital certificates are assigned, and ongoing audit process is in place to monitor and proactively renew with the PSAP and/or CPE Vendor prior to expiration. While the certs carry 3-year expiration terms, AT&T's business process is to renew at approximately the 2-year mark to avoid potential lapses. AT&T renews the certs and provides them via encrypted email to the PSAP and/or CPE vendor for installation. To add an additional layer of vigilance, AT&T continually monitors expiry dates and notifies PSAPS/CPE vendors of impending expirations 90 days in advance. If not renewed 60 days prior to expiration, AT&T sends another notice. Should the certs still be pending renewal 30 days before the expiration date, AT&T will again escalate the matter to the PSAP/CPE Vendor and proactively renew the certs, so they are available to be sent at a moment's notice. The digital certificates are active when sent, and are available to be loaded, configured and activated when the PSAP and CPE vendor is ready to do so. This requires no additional configuration, testing or support from AT&T – but AT&T is always available for additional questions or concerns. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
ATT	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Secure Software Design/Testing** **Questions 131**: Is your organization outsourcing any aspect of the service to a third party? **Vendor Response**: Yes **E911 Response:** E911 requires additional cybersecurity information on these third parties. What is their cyber-relationship with the vendor? What cyber agreements are in place to protect customer data? **AT&T Clarifying Response:** For the AT&T ESInet solution, we have implemented a defense-in-depth information security methodology, with infrastructure in place to control and monitor network interfaces and traffic and limit connectivity to known, trusted sources. Implementation of security infrastructure including firewalls, IPS/IDS, anti-virus/malware agents, and

	centralized event logging allow for granular visibility and control across the network. Internal vulnerability monitoring has been implemented across our network, conducting scans on monthly basis, on-demand, or when major changes have been made to infrastructure elements. In addition to internal vulnerability monitoring, we complete annual penetration testing using a third-party security vendor to identify potential exposures and vulnerabilities present on AT&T ESInet systems. The testing is designed to simulate an attack from a malicious outsider against externally networked systems. The testing methodology used consists of multiple phases including scanning infrastructure for vulnerabilities and attempting to exploit vulnerabilities. Vulnerabilities discovered during penetration testing are mitigated and remediation testing is planned with the penetration testing vendor to validate the mitigation steps that have been implemented. Regarding agreements we have in place, AT&T requires that suppliers contractually adhere to AT&T Supplier Information Security Requirements (SISR). These requirements apply when suppliers: • Handle or access AT&T's confidential or proprietary data, including customer information. • Access AT&T's Information Resources, such as systems, networks, or applications. • Provide or support AT&T-branded services using non-AT&T technologies (e.g., cloud services, APIs, mobile platforms). • Develop or customize software for AT&T. • Host or develop websites for AT&T. AT&T Chief Security Office (CSO) has verified that Intrado complies with AT&T's SISR policy. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.

Vendor Name	**Comments**
INdigital	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES /** **Question 1**: REQUIRED RESPONSE: Will your organization provide SOFTWARE-AS-A-SERVICE (SaaS)? (e.g. Software- as-a-service/SaaS, application, website) **Vendor Response:** Yes, Our Texty, 911Logix, and some of the NGALI solutions are hosted web applications. **E911 Response:** Please provide additional information on which components "some" are hosted

	Vendor Response: 1). Texty is a secure, private cloud hosted application platform that is deployed as a secure user level permission based Chrome browser application or via secure direct integration with CHE or CAD systems. Web access uses MFA + TLS security. 2). 911 Logix ingests SIP-REC data from the ESiNet using Microsoft Azure government services. Access to the dashboard and reporting functions use MFA + TLS security. 3). NGALI is a secure, private cloud hosted application platform that is deployed as a user level permissions based Chrome browser application. Access uses MFA + TLS security. All SaaS functions are compliant with INdigital's security posture architecture. A copy of INdigital's security plan is attached as Appendix **INdigital #1 Section 1 - Security Plan** **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
INdigital	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES /** **Question 3:** REQUIRED RESPONSE: Will your organization provide APPLICATION DEVELOPMENT SERVICES? (e.g. on-premise, mobile, web, or other custom code) **Vendor Response:** Yes, Many of the supporting applications are custom developed **E911 Response:** E911 requires the vendor who provides custom coding options to implementing robust cybersecurity measures is essential for safeguarding application development services, whether they are on-premise, mobile, web, or custom code. Provide which best practices for securing application development the vendor follows. **Vendor Response:** INdigital's SaaS hosting and FE application development services are fully compliant with INdigital's security posture architecture. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
INdigital	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / External Parties** **Questions 23**: Will third parties, such as IT service providers have access to the County's data that is stored or transmitted by your organization? **Vendor Response**: Yes, OTM Cyber is the third party security vendor responsible for monitoring traffic and systems at our Florida supporting data centers; Public Safety Networks of America is the developer and provider of our MIS solution 911 Logix **E911 Response:** E911 requires that any privacy / data sharing agreements must ensure that the client data is secure, the vendor should have that language with all 3rd party IT service providers? **Vendor Response**: INdigital security posture compliant contractual security requirements in place with both PSNA (911 Logix) and OTM Cyber (third party monitoring.)

	E911 Response: E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
INdigital	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / External Parties** **Questions 26**: Will third parties, such as IT service providers have access to the County's data that is stored or transmitted by your organization? **Vendor Response**: Yes, Spain **E911 Response:** E911 requires information on these external parties: What is their relationship with INdigital? What agreements are in place to protect customer data? Response: INdigital maintains a security posture compliant relationship with the Madrid software development team. All IT repositories, access methods, and other protocols are enforced by INdigital with Zaleos. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
INdigital	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Regulatory Compliance** **Questions 35**: Does your organization have a documented process to identify new laws and regulations with IT security implications (e.g., FIPA, new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)? **Question 36:** Yes, Has your organization experienced a data breach within the past five years that legally required reporting under applicable law? **Vendor Response**: INdigital has members focused on regulatory compliance and members partaking in groups and organizations such as DHS CISA and the COMM ISAC **E911 Response:** Is your organization incompliance with FLHB7055 and the FLDS reporting requirements?

	Vendor Response: We are generally made aware of new laws and regulations by the in-state 911 program and our customers. INdigital has reviewed the 2025 Florida Statute, Title XXXIII section / chapter 501.171, (submitted) which we assume is the FIPA requirement inquired upon. These requirements are similar to other federal requirements with which INdigital complies. As noted in our response, INdigital does monitor and identify emerging security requirements in North America. The FIPA statute will be added to our overall security posture and compliance processes with the assessment that the primary areas of a compliant security posture are: (A.) 501.171; (1); (g); 1; (a); (VII) Any information regarding an individual's geolocation. " INdigital currently includes this requirement in our internal security posture and in our third party contractual arrangements. (B.) 501.171; (2); (h) "Third-party agent" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity." INdigital will make these statutory citations a part of our security posture and operating policies, and establish the statutory compliance requirement. **Question 36:** Yes, Has your organization experienced a data breach within the past five years that legally required reporting under applicable law? Response: INdigital has not had any data breaches. **Vendor Response**: INdigital has members focused on regulatory compliance and members partaking in groups and organizations such as DHS CISA and the COMM ISAC **E911 Response:** Is your organization in compliance with FLBS7055 and the FLDS reporting requirements? **Vendor Response**: INdigital has reviewed FLDS publication "The Local Government Cybersecurity Resource Packet, 2025 V2.0" as well as Florida Statutes section 282.3185(4) - Local government cybersecurity, Cybersecurity Standards. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
INdigital	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Crypto Materials and Key Management** **Questions 125**: Does your organization have a centralized key management program in place (e.g., any Public Key Infrastructure (PKI), Hardware Security Module (HSM)-based or not, etc.) to issue certificates needed for products and cloud service infrastructure? **Vendor Response**: Yes. **E911 Response:** E911 requires documentation on your PKI / CA infrastructure and how you handle certificate generation, renewal and revocation.

	Vendor Response: INdigital follows the PKI / CA protocols and procedures set out in the NENA i3 standard. While a NENA managed service for this method of security has not yet entered the marketplace, the need to provide and support security measures is here now. Given that PKI / CA requirements are well known as a common commodity, the method of efficient management of these security measures is well known. Response: INdigital has attached Appendix **INdigital #6 PKI Management (Q 125)** for Broward County's review. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
INdigital	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Secure Software Design/Testing** **Questions 131**: Is your organization outsourcing any aspect of the service to a third party? **Vendor Response**: Yes **E911 Response:** E911 requires additional cybersecurity information on these third parties. What is their cyber-relationship with the vendor? What cyber agreements are in place to protect customer data? **Vendor Response**: INdigital has third party relationships with the following parties: 1). Zaleos Engineering, Madrid, Spain. Zaleos is an embedded software development firm that is fully adherent to INdigital's security posture. Compliance measures are in the intercompany contract and operating Agreements. 2). PSNA - 911 Logix is a Florida based company that has access to INdigital's data lake for dashboarding and reporting functions. In some jurisdictions, data from the CHE and CAD are also ingested to provide a more comprehensive reporting platform used by state 911 programs and local PSAPs. Access to the functions of 911 Logix are set at the user permission levels at the direction of the local 911 authority. 3). GIS data - With the exception of local policies that may apply, (grey box or restricted areas) the data used by INdigital is typically publicly available information from data aggregators - usually with a relationship to the authoritative GIS data source. The primary focus of security is to prevent the compromise of the routing data that could result in mis-routed calls or texts. In the proposed solution, INdigital has full custody and control of the GIS data used for SaaS to Broward County, and its use is at Broward's direction and guidance. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.

Vendor Name	Comments
Motorola	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / External Parties** **Questions 26**: "Does your organization utilize any off-shore resources for development? Provide location(s)." **Vendor Response**: Yes, Krakow, Poland **E911 Response:** E911 requires information on these external parties: What is their relationship with Intrado? What agreements are in place to protect customer data? **Motorola Response 10/7/25:** To clarify, one of Motorola's development operations in Krakow is staffed by Motorola-badged employees and is not considered an external party in the context of third-party access to the County's data. These employees are covered under Motorola's standard employee policies and procedures, with the same protections afforded to US-based employees. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
Motorola	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Regulatory Compliance** **Motorola UPDATED Questions 35**: Does your organization have a documented process to identify new laws and regulations with IT security implications (e.g., FIPA, new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)? **Vendor Response**: Yes **Motorola Response 10/7/25:** Motorola has received and will comply with the reporting requirements defined in 2022 CS/HB 7055, as well as the Florida Digital Service requirements. **Question 36:** Has your organization experienced a data breach within the past five years that legally required reporting under applicable law? **Vendor Response**: No **E911 Response:** Is your organization familiar with FLBS7055 and the FLDS reporting requirements?

	Motorola Response 10/7/25: Motorola has not experienced a data breach within the past five years. We are proud to manage our cybersecurity needs with our own dedicated division, formerly known as Delta Risk, a practice that sets us apart from many vendors who outsource these critical functions. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
Motorola	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Network Defense and Host Intrusion Prevention Systems** **Questions 86**: Does your organization have any Intrusion Protection System (IPS) in place for your environment? **Vendor Response**: Yes **E911 Response:** E911 requires the cyber-related information on the vendor's IPS solution. Does the vendor support integration to the County E911 SIEM? **Motorola Response 10/7/25:** Motorola Solutions is prepared to integrate with Broward County's Security Information and Event Management (SIEM) system. However, to provide specific details regarding this integration, we will need to know which SIEM platform the County is currently utilizing. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.
Motorola	**SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES / Secure Software Design/Testing** **Questions 131**: Is your organization outsourcing any aspect of the service to a third party? **Vendor Response:** Yes, As a cloud service, cloud hosting infrastructure is managed by a third-party cloud provider **E911 Response:** E911 requires additional cybersecurity information on these third parties. What is their cyber-relationship with the vendor? What cyber agreements are in place to protect customer data? **Motorola Response 10/7/25:** 1. What is their cyber-relationship with the vendor? Our cyber-relationship with our cloud service providers, Amazon Web Services (AWS) and Microsoft Azure, is formally defined by the industry-standard Shared Responsibility Model. This model establishes a clear division of security obligations:

	The Cloud Vendor's Responsibility (Security OF the Cloud): AWS and Azure are responsible for protecting the underlying global infrastructure. This includes the physical security of their data centers, the hardware, the networking, and the virtualization layer. Our Responsibility (Security IN the Cloud): As their customer, we are responsible for everything we deploy on their infrastructure. This includes securing our application code, managing user access and identity controls, encrypting customer data, configuring firewalls and networks, and maintaining the security of the operating systems. In this relationship, we act as a strategic partner and direct customer, leveraging their highly secure and compliant government cloud platforms (AWS GovCloud and Azure Government) as the foundation upon which we build and manage our secure NG9-1-1 solution. 2. What cyber agreements are in place to protect customer data? To protect customer data, we have a comprehensive framework of legal and operational agreements in place with both AWS and Azure. These include: Enterprise Customer Agreement: The master contract that governs the overall business relationship and terms of service. Data Processing Addendum (DPA): A legally binding addendum that dictates the specific roles and responsibilities for processing and securing customer data. It ensures the vendors adhere to the stringent data protection and privacy standards required for sensitive E911 information. Service Level Agreements (SLAs): Contractual commitments from the vendors that guarantee specific levels of service availability and uptime (e.g., 99.99% or higher), which is critical for the resilience of our security and operations. **E911 Response:** E911 standard requires County Data processed, transmitted, or stored by Contractor or in the Contractor's system is not accessed, transmitted, or stored outside the United States.