

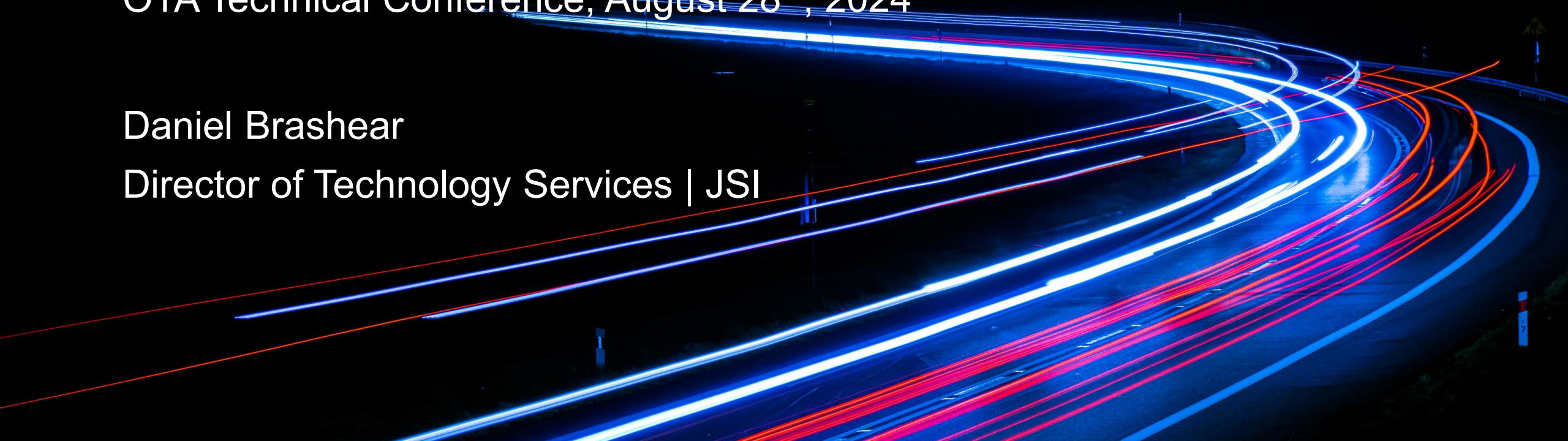
Cybersecurity & Voice Evolution

A Look at Current and Emerging Developments

OTA Technical Conference, August 28th, 2024

Daniel Brashear

Director of Technology Services | JSI



Agenda

Cyber Trends

Cyber Requirements

Uncertainty in Voice

Certainty in Voice

Wrap-Up/Questions



Cyber Trends

U.S. NEWS

Rural Texas towns report cyberattacks that caused one water system to overflow

- Water systems the focus of attacks targeting three rural towns
 - Systems had to be moved to manual control; one experienced an overflow
 - Fortunately, drinking water was not compromised, but this highlights that "small" entities are often targeted due to tendency toward underfunding in cyber defense



Cyber Trends

- CrowdStrike – Faulty Update Leads to Worldwide Outages
 - Roughly 8.5 million systems crashed and were unable to restart properly
 - Probably the largest IT outage ever with financial damages upwards of **\$10 billion**
 - Particularly scary as an otherwise reputable and trusted vendor caused massive issues for companies who were in fact following best-practices by running this sort of software and keeping systems up to date
 - Highlights that issues can occur with even the best of vendors and that it is **critical to conduct due diligence and incidence response planning/testing**

Cyber Trends

- CDK Hack – Ransomware event affecting auto dealership software firm
 - Unclear how ransomware was installed on the network, but it is typically done via phishing emails or device vulnerability exploitation
 - CDK likely paid 387 bitcoins (~\$25M) in ransom
 - Affected nearly 15,000 businesses with an estimated nearly \$1B in losses
- How do you safeguard against ransomware?

PREVENTION

- Network hardening
- Security awareness training
- Vulnerability management

RESPONSE

- Backups
- Cybersecurity insurance
- Incident response planning
- Third-party relationships



Cyber Requirements


Is your cyber posture ready for a BEAD application and award?





BEAD NOFO Cybersecurity Requirements

Prior to allocating any funds to a subgrantee, an Eligible Entity must require a prospective subgrantee to attest to 4 requirements relating to cybersecurity.

 BEAD NOFO Section IV.C.2.c.vi Program Structure, Sequencing and Requirements; Program Requirements; Obligations for Subgrantees Deploying Network Projects; Service Obligations; Cybersecurity and Supply Chain Risk Management



The prospective subgrantee has a **cybersecurity risk management plan** (the plan) **in place** that is *either*:

- a. **operational**, if the prospective subgrantee is providing **service prior to the award of the grant**; or
- b. **ready to be operationalized upon providing service**, if the prospective subgrantee is **not yet providing service** prior to the grant award;



The plan reflects the latest version of the **National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity** (currently Version 1.1) and the **standards and controls set forth in Executive Order 14028** and specifies the security and privacy controls being implemented;



The plan will be **reevaluated and updated on a periodic basis** and as events warrant; and




The **plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes** to the plan, a **new version will be submitted to the Eligible Entity within 30 days.** The Eligible Entity must provide a subgrantee’s plan to NTIA upon NTIA’s request.



Supply Chain Risk Management (SCRM) Requirements

Prior to allocating any funds to a subgrantee, an Eligible Entity must require a prospective subgrantee to attest to 4 requirements relating to SCRM.

 BEAD NOFO Section IV.C.2.c.vi Program Structure, Sequencing and Requirements; Program Requirements; Obligations for Subgrantees Deploying Network Projects; Service Obligations; Cybersecurity and Supply Chain Risk Management



The prospective subgrantee has a **SCRM plan in place** that is *either*:

- a. **operational**, if the prospective subgrantee is **already providing service** at the time of the grant; or
- b. **ready to be operationalized upon providing service**, if the prospective subgrantee is **not yet providing service** at the time of grant award;



The plan is based upon the **key practices discussed** in the **NIST publication NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry** and related SCRM guidance from NIST, including **NIST 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations** and specifies the supply chain risk management controls being implemented;



The plan will be **reevaluated and updated on a periodic basis** and as events warrant; and



The **plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes** to the plan, a **new version will be submitted to the Eligible Entity within 30 days.** The Eligible Entity must provide a subgrantee’s plan to NTIA upon NTIA’s request.



Cyber Requirements

- Essential Info
 - Every state, except for Nevada, has so far required that you at least **certify** you have these plans in place during the **pre-qualification** process
 - About 50% of the states have required that you also **upload** a copy of your plans during the **pre-qualification** process
 - Note: Some of the portals don't make this obvious until you have already clicked to certify you have a plan (then the upload box appears)
 - JSI strongly recommends you get started on these plans immediately if you are considering a BEAD application



Cyber Requirements

- Some Good News!
 - If you developed plans for EA-CAM, the requirements are identical
 - Requirements for Reconnect have been somewhat less stringent, but you may be close if you have plans for Reconnect—JSI can review your plans for you
 - If you used JSI’s plan templates for EA-CAM or Reconnect, you should be set
 - If you need to get plans in place, JSI can help you get this knocked out quickly using our customizable plan templates
- Takeaways
 - Virtually every funding opportunity at the federal and state level, whether grant or ongoing subsidy, looks to be converging on similar requirements for cyber programs
 - The right time to start working on your cyber plans is *now*

Cyber Requirements

- CISA / CIRCIA NPRM on Incident Reporting
 - Proposes to require covered entities, including communications providers, to file reports if affected by a “covered cyber incident”
 - A “covered cyber incident” is somewhat clarified as a “substantial cyber incident” with any of the following impacts:
 - Substantial Loss of Confidentiality, Integrity or Availability
 - Serious Impact on Safety and Resiliency of Operational Systems and Processes
 - Disruption of Ability to Engage in Business or Industrial Operations
 - Unauthorized Access Facilitated Through or Caused by a: (1) Compromise of a CSP, Managed Service Provider, or Other Third-Party Data Hosting Provider, or (2) Supply Chain Compromise

Cyber Requirements

- CISA / CIRCIA NPRM on Incident Reporting
 - Report types and timeframes
 - Covered Cyber Incident Report – 72hrs after incident
 - Ransom Payment Report – 24hrs after payment made
 - Joint Covered Cyber Incident and Ransom Payment Report – 72hrs after incident (satisfies both requirements in one report)
 - Supplemental Reports – “promptly” upon availability of new info (24hrs)
- Comments Filed Propose Consideration for:
 - Minimize the reporting burden for small providers (e.g., less detail and fewer updates)
 - Focus should be on recovery and threat reduction, not on reporting; as such, definitions need to be tightened and thresholds relaxed
 - Minimize duplicative reporting, limit retention periods to practical times, protect confidentiality

Other Cyber Related News

- FCC's Schools and Libraries Cybersecurity Pilot Program
 - Expected to open for applications this Fall
 - Will provide up to \$200 million in funding to schools and libraries
 - This funding can be used to purchase a wide range of cybersecurity services and equipment including:
 - Next-generation firewalls
 - Vulnerability scans
 - Endpoint protection
 - 24/7 Security Operations Center (SOC) monitoring
 - Distributed-Denial-of-Service (DDoS) protection
- Service providers can help implement eligible equipment and services (JSI can help you!)

Uncertainty in Voice



Uncertainty in Voice

- TDM Costs Rising While Becoming Less Reliable
 - SS7 signaling solutions skyrocketing while becoming a cause of some major outages
 - PSTN connectivity (particularly for CLECs)
 - ...and yet the RBOC tandems still won't connect via SIP
- Microsoft/Metaswitch
 - Previous layoffs were already driving inefficiency in new deployments & upgrades; latest layoffs have hit the professional services and sales org heavily
 - Microsoft has indicated they prefer to only provide the infrastructure (Azure) for voice solutions going forward; will they sell to someone? Is that a good thing if so?
 - EOL/EOS dates not yet certain, though it does seem likely that anything not currently EOL will survive at least as long as the current latest dates in 2029

Uncertainty in Voice

- Skilled Workforce
 - Knowledgeable switching techs are getting hard to find
- New Costs for Providers
 - STIR/SHAKEN
 - Now deployed for those with IP in their voice networks, but some do not
 - What about TDM going forward?
 - NG911
 - In varying stages of deployment across the US—FCC order seeks to address this
 - OSPs received some “wins” relative to the original NPRM; some recovery mechanisms exist, but ultimately OSPs are responsible for implementing

Certainty in Voice



Certainty in Voice

- SIGTRAN-based SS7 solutions are available; costs are still higher overall than they once were as this market has become less competitive recently, but are generally less costly and more reliable than TDM-based solutions
- IP Tandems have emerged as a potential solution (with a cost)
- Cloud switching is maturing with several good, reliable options now available
- NECA is helping to smooth the path to cloud switching via clarifications on switching requirements within the LATA
- JSI can help navigate all the possible combinations of options to ensure your switching solution going forward is both economical and robust (ask us about *Voice Evolution!*)

Wrap-up/Questions

Daniel Brashear

Director of Technology Services | JSI

Office: 806-866-9900

Mobile: 575-309-4904

daniel.brashear@jsitel.com

Robert Whitlock

Director | JSI

Mobile: 918-809-9924

robert.whitlock@jsitel.com