Conceptual Architecture for Cyber Safe Communities

Securing America’s critical infrastructure through local governance

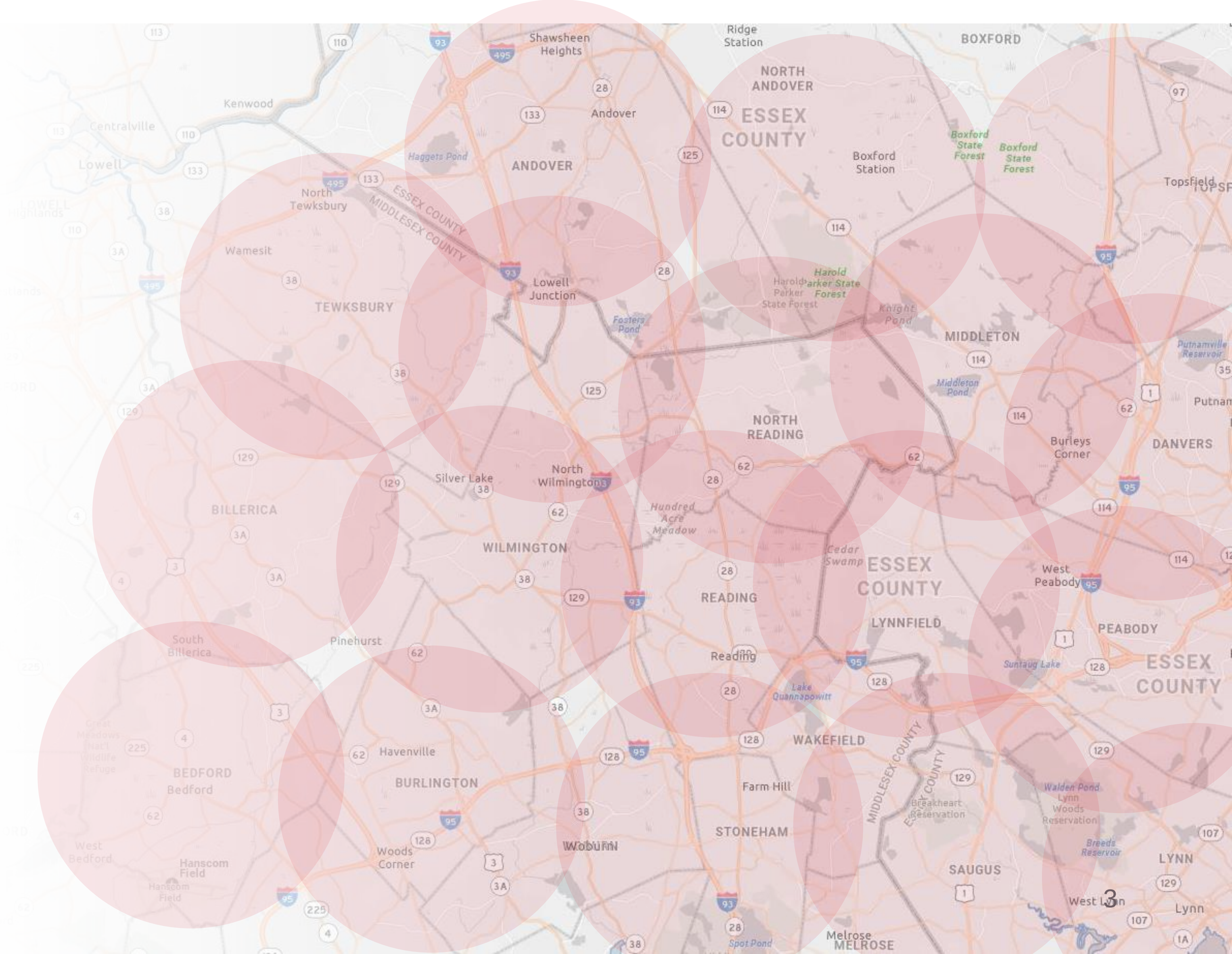
RTX Technology Research Center

Fred Jones
Senior Technical Fellow
Frederick.Jones@rtx.com

A novel regulatory framework for creating localized cyber safe communities

Concept Goal: Develop cybersecurity best practices and technologies across the U.S. that can be controlled and governed in local cyber districts.

- Cyber districts would be roughly approximate to zip code boundaries.
- Residents in each district would have access to a community-owned and -operated secure LAN.
- Pooled risk and local data ownership/control will drive resiliency on a national scale.



Cyber district LANs

Concept: District LANs would be structured like those of large corporations.

- Supplements general purpose networks.
- Intended for high-consequence, regulated transactions (e.g., finance and medical data).
- Provides email and protected web browsing for district residents.
- Access via multi-factor authentication.
- All activity monitored.

Models for cyber district governance

The Fire District Model

- Community-owned, pooled-risk organizations.
- Geographic boundaries.
- Funded via local property taxes.
- Staffed by volunteers and professionals.
- Supports community awareness programs.
- Defines building codes.
- Provides incident response services.
- Coordinates cross-district response.

Models for cyber district governance

U.S. Postal Inspection Service (USPIS)

- Oldest law enforcement team in the U.S.
- Geographic dispersal of facilities.
- Authority defined by federal regulatory code.
- Ensures confidentiality, integrity and availability of delivery.
- Enables transmission of secret-level classified materials.
- Penalties for malicious activities (unauthorized opening, tampering, obstruction, counterfeiting, misrepresentation, dangerous/illegal materials).

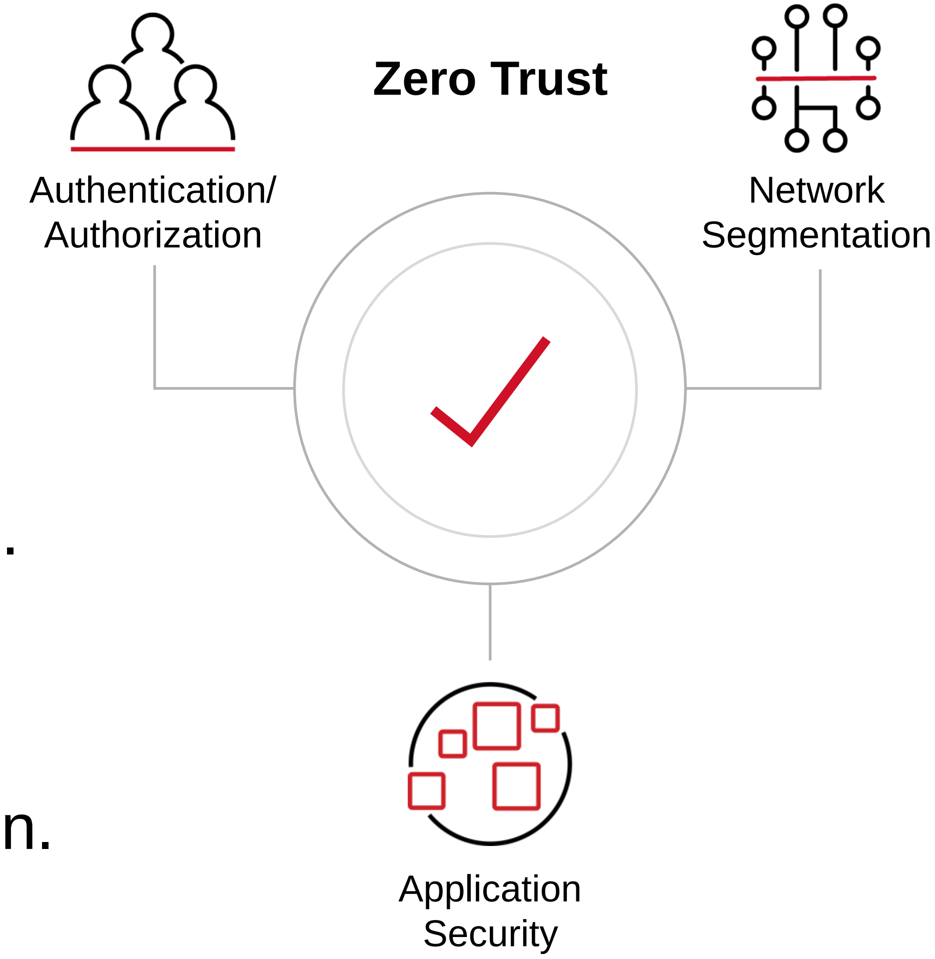
Identical missions and tenets for cyber districts concept

- Geographic boundaries.
- Funded via local property taxes.
- Staffed by local municipalities.
- Cyber “building” codes define minimum required measures for connected systems.

- Supports critical infrastructure: schools, fire, police, hospitals, water, electric, government, etc.
- Critical infrastructure data resides in local districts.

Critical components to realizing the vision

- National standards to govern the flow of data between districts.
- Zero-trust network security.
- Identity access management.
- National digital identity system that collaborates with local and state governments.
- Support from the NIST, USPS/USPIS, FCC, DOD, DHS and several other agencies.
- Collaboration with Smart City concept adoption.



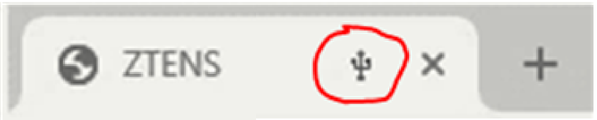
Establishing a national network of secure facilities to enable classified electronic communication

Secure Facilities at Airports Concept

- ICD 705 facility compliance within the security perimeter of airports.
- Guards and additional identity checks prior to entry.
- Special boarding passes for passage through TSA checkpoints and scheduling time in the airport.
- Access to secure communication systems: video conferencing, email and websites.
- Quick participation in classified discussions for cleared individuals and critical infrastructure operators.
- Timely dissemination of threat intelligence.

ZTENS

Zero Trust Endpoint
Network Security



Chrome / Edge Browser

+

ZTENS

Internet

- Low-cost, commodity hardware device with Bluetooth, Wi-Fi & USB connectivity
- ZTENS device implements all network communications for a browser tab
- Browser connects to ZTENS device via either Web Bluetooth or WebUSB
- Eliminates dependence on most public network security services
- Moving network security into domain of tamper-evident/tamper-resistant technology

✓ Bespoke Network Connectivity (not general purpose)
✓ Eliminate phishing attacks
✓ Resistance to Distributed Denial of Service (DDoS) attacks
✓ Remove DNS, Certificate Authority, Public Key dependency
✓ Ephemeral IPv6 – time+device dependent address:port
✓ Enabler to Web3 Technology Adoption
✓ Anonymized routing, TOR (The Onion Router, Dark Web)
✓ Multi-Pathway Packet Routing (eg split 5G + WiFi)
✓ Hardware security features enable user identity attribution
✓ Endpoint network data analysis (audits, insider threat mitigation)
✓ Quantum Computing Resistant, hardware-enabled cryptography
✓ Novel integration of cyber and hardware security
✓ Combined multi-factor authentication & VPN solution
✓ Raytheon Patented Technology (US20220239697A1)

ZTENS is a new approach to private, secure network communications (Raytheon patent)

It’s a vision that demands success

Primary objective: supporting national security interests.

The most effective route to protecting the U.S.’ critical infrastructure and communities is by creating cyber districts through federated, locally controlled segmented networks.

The models are in place to show us the way. A team of industry and government partners can make it happen.

Thank you.