TESTIMONY TO SENATE GOVERNMENT AND VETERANS AFFAIRS REGARDING BILL 1417

© Gerald Blank

www.jerryblank.us

Kevin Ford – Chief Information Security Officer NDIT
3/10/2021

NORTH
Dakota
Be Legendary.™

The State and Local Cyber Problem

- State and local governments have the same problems
- We aren't addressing our problems in coordinated way

"States and localities are stronger when they share awareness and resources, thereby fostering resilience beyond any individual legal jurisdiction." - DHS

National Adoption of Mutual Aid

"The most consequential cyber challenges require resources beyond the capacity of the federal government or that of a single state."

"Just as state and regional incidents in the physical world are dealt with by FEMA, states, and private surge arrangements for mutual aid so too should cyber challenges be handled effectively through a spectrum of arrangements."

From: HOMELAND SECURITY ADVISORY COUNCIL FINAL REPORT OF THE STATE, LOCAL, TRIBAL AND TERRITORIAL CYBERSECURITY SUBCOMMITTEE, available https://www.dhs.gov/sites/default/files/publications/sltt_final_report_signed.pdf

Memorandums of Understanding for Cybersecurity Information Sharing

What are they targeting?

Who are they?

How do they act?

How do we beat them?

Personal Data is not Shared

Mutual Aid Agreements

Access to varied toolsets and capabilities

Swarming to most acute site of an attack before it spreads

Coordination of actions to beat attackers, not just repel them

Promotes overall network health by exposing it to fewer attacks from partners

Future Opportunities

COVID relief grants tied to Cyber Mutual Aid

DHS arranged bulk purchase vehicles for commonly used cyber essentials

Multiple bills and draft bills include cybersecurity funds for mutual aid

Multistate purchasing for bulk tools

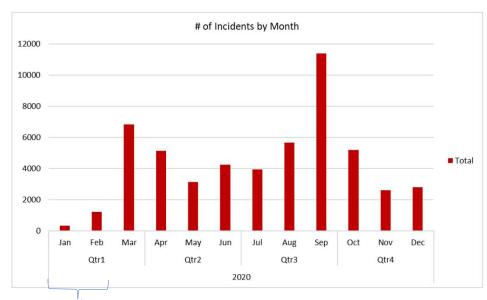# North Dakota Tribal Governments

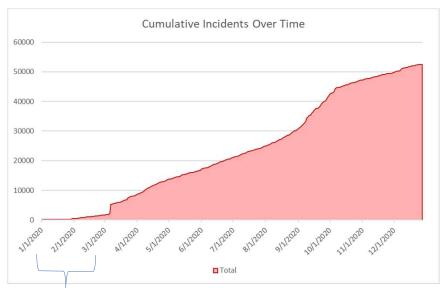# Appendix

External Threats

North Dakota receives over 177 Million detected attacks per month[1] from external threats including:
- Nation States,
- Corporate Espionage, and
- Organized Crime Syndicates.

1. Based on ¼ Sampling of 2020 Firewall logs from June 2020, August 2020, October 2020, and Last 30 days (as of December 20, 2020) - Logs available in appendix

52,415 Cyber Incidents (March 2020 to Nov 2020)

# of Incidents by Month

Most tools were not integrated, count is artificially low

Cumulative Incidents Over Time

Most tools were not integrated, count is artificially low

Incidents based on Cortex XSOAR Incidents between 01/01/2020 – 12/28/2020. This number is artificially low as all alerts/events were not being ingested into XSOAR prior to March 2020.