– Appendix F

As announced in December 2022, NIRMA joined forces with NACO, MIPS, Applied Connective Technologies, and Bytes Managed IT in a **County Network Security Cooperative** aimed at encouraging cyber security best practices specifically for counties.

With added input from other governmental representatives including from CISA and the State of Nebraska, the Cooperative developed the guidance document that follows, which is intended to be printed as a double-sided single page.

All vendor members of the Cooperative have agreed to abide by and be capable of providing counties with the services identified on the guidance document.

To mitigate the risk of cyber-related fraud and claims, NIRMA encourages its members to implement, at a minimum, the services identified in the "Basic" column of this guidance document, and strive toward implementing those services in the "Better" and "Best" columns.

Many of the services identified on the Cooperative's guidance document are described in greater detail elsewhere in this Toolkit. See the infographic on p. 32 of this Toolkit for a visual of how many of these components fit into a layered approach to cyber security.

Managed IT and Cyber Services

The below services and recommendations are provided to serve as a guide to assess your IT and Cyber security preparedness. Further descriptions and solutions that meet the recommendations are provided on the backside as examples, other solutions may meet suggested criteria.

SERVICES	BASIC	BETTER	BEST
.gov Email	✓	✓	✓
Email Security / CSAT	✓	✓	✓
County Network (OCIO separation)	✓	✓	✓
Wireless Networks	✓	✓	✓
Firewall - Licensed NGFW	✓	✓	✓
Vulnerability Management - Perimeter	✓	✓	✓
Endpoint Protection	✓	✓	✓
Patch Management	✓	✓	✓
MFA (VPN and Email)	✓	✓	✓
Backup	✓	✓	✓
Password Manager	✓	✓	✓
County Network / System Authentication	✓	✓	✓
M365 Backup and Archiving	✓	✓	✓
Endpoint Protection - Advanced		✓	✓
Backup - Advanced		✓	✓
MFA - Advanced		✓	✓
Vulnerability Management - Endpoint			✓
Log Analysis (SIEM) w/ SOC Monitoring			✓
Endpoint Protection w/ SOC Monitoring			✓
IT Services - Standard w/ Helpdesk	✓	✓	✓
IT Services - Premium w/ Onsite		✓	✓
IT Services - Internal IT Supplemental			✓
IT Services - Quarterly Reviews vCIO			✓
Centralized Network Environment	✓	✓	✓
Secured Physical IT Environment		✓	✓
Temperature Controlled IT Environment		✓	✓

Disclaimer: This document was approved by the County Network Security Cooperative and reflects current guidance which will be subject to periodic updates to reflect changes in the evolving cyber security environment.

NACO Nebraska Association of County Officials

NIRMA Serving County Government

v1.0 Created 12/01/2022

- .gov Email: Microsoft Exchange online or Google Workspace - required for all County Staff and Supervisors.
- Email Security / CSAT (cyber security awareness training): Suggested platforms include scanning and anti-phishing functionality. Suggested vendors: IronScales, Knowbe4, Barracuda, ProofPoint, etc
- County Network (OCIO separation): All County owned systems connected to separate County LAN, VLAN segregation of CJIS, proper State application routing via OCIO firewall. OCIO (Office of the Chief Information Officer - State of Nebraska)
- Wireless Networks: Secure and separate guest and private networks. Cloud managed platform with portal login or frequent password rotation.
- Firewall - Licensed NGFW (next generation firewall appliance) with cyber licensing. Suggested vendors: Fortinet, WatchGuard, SonicWALL, Cisco Meraki, Palo Alto
- Vulnerability Management - Perimeter: Perimeter network scanning. Suggested vendors: CISA CyHy, Qualys.
- Endpoint Protection: Managed commercial endpoint protection. Portal management and enforcement. Suggested vendors: BitDefender, Webroot, Cylance, SentinelOne, Defender, ESET, Sophos.
- Patch Management: Enforced and frequent patching of OS and critical 3rd party softwares: WSUS, RMM (ie: Ninja RMM, ConnectWise Control, Atera).
- MFA (multi factor authentication): Enforcement of MFA on all remote access and County email platforms.
- Backup: Minimum onsite disk rotation backup (ie: Shadow Protect by MIPS). Backup of all critical data.
- Backup - Advanced: Automated cloud backup system with onsite/cloud storage. Monitored. Includes business continuity features. Suggested vendors: Axcient, Veeam, Datto.
- County Network / System Authentication: User of local Microsoft active directory services or Azure active directory for County desktops, laptops and servers.
- Endpoint Protection - Advanced: Advanced endpoint protection with detection/response features. Suggested vendors: SentinelOne, CylancePROTECT, Crowdstrike, Huntress.
- Password Manager: Managed commercial password manager for all County staff. Suggested vendors: LastPass, Keeper, BitWarden.
- M365 Backup and Archiving: Backup of cloud hosted email and document systems. Suggested vendors: DropSuite, x360 Cloud.
- MFA - Advanced: Managed advanced commercial MFA platform. MFA on key infrastructure: Servers, Firewalls. Suggested vendors: DUO.
- Vulnerability Management - Endpoint: Internal network and endpoint vulnerability scanning and assessment. Suggested vendors: CISA, Qualys.
- Log Analysis (SIEM) w/ SOC Monitoring: Managed log analysis for servers, Azure, firewall and optionally endpoints. Suggested vendors: EventTracker, ConnectWise SIEM.
- Endpoint Protection w/ SOC Monitoring: Managed endpoint protection to include security operations center monitoring, alerting, response and remediation services.
- Centralized Network Environment: Ethernet cabling home run to centralized IT rack(s) to allow for proper network VLAN (virtual LAN) and LAN segregation (ie, private county, private state, CJIS, public networks) via managed network switching and firewall equipment.