New Jersey Cybersecurity & Communications Integration Cell

Defending Our Digital Density.

@NJCybersecurity

cyber.nj.gov

NJCCIC@cyber.nj.gov

The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) is known as the Division of Cybersecurity of the New Jersey Office of Homeland Security and Preparedness (NJOHSP). NJOHSP helps to direct prevention, detection, protection, response, and recovery planning, not only at the State level, but also at the regional and national levels with our varied partners. NJOHSP is comprised of four Divisions: Intelligence, Policy and Planning, Cybersecurity, and Administration.

What is the NJCCIC?

The State's clearinghouse for information sharing, threat intelligence, best practices, and incident response

- Consists of OIT, NJSP, OHSP and Federal Partners
- Multi-disciplinary, holistic approach to cybersecurity
- Promote statewide awareness of cyber threats
- Facilitate widespread adoption of best practices
- Collaborate with public and private sectors with the goal of making NJ more resilient to cyber attacks

General Threat Trends

- External threat environment increasing
- Credential compromise is the key to the kingdom
  - Phishing email is the #1 attack vector for credential compromise
    - 91% of all phishing emails attributed to organized crime groups
    - Purpose of phishing is to gain a foothold and compromise credentials
    - CEO/CFO whaling losses increased exponentially
  - Vulnerability exploitation
    - Avg. 30 days before a known vulnerability is exploited
    - Most attacks focus on old unpatched vulnerabilities
- Distributed Denial of Service Attacks
- Crimeware/Ransomware is rising – as payments are made ransomware will continue to increase in frequency and business impact.
- Cyber Hygiene

"Think Like a Criminal" Framework

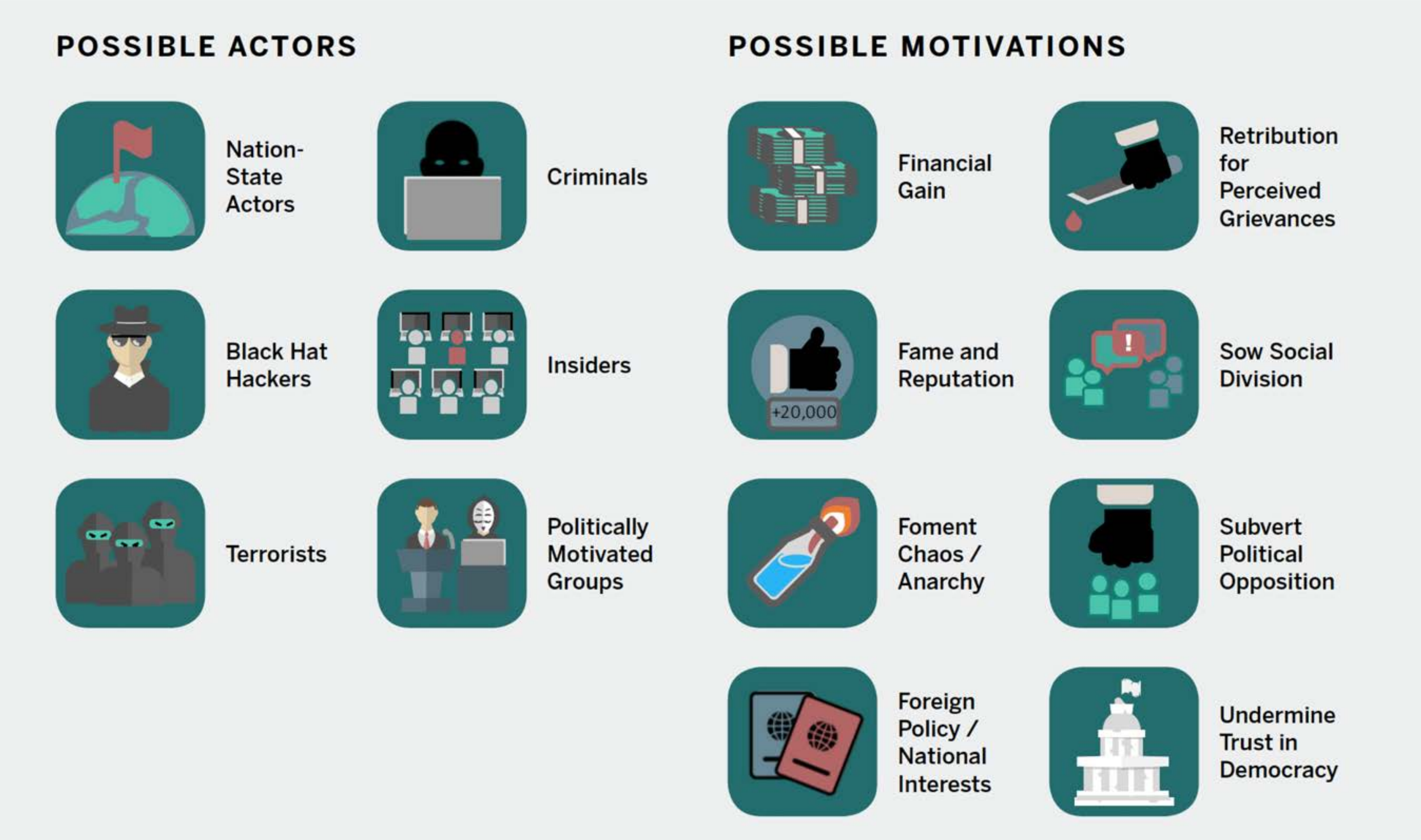
Attacker

Means

Motive

Opportunity

The Who And The Why



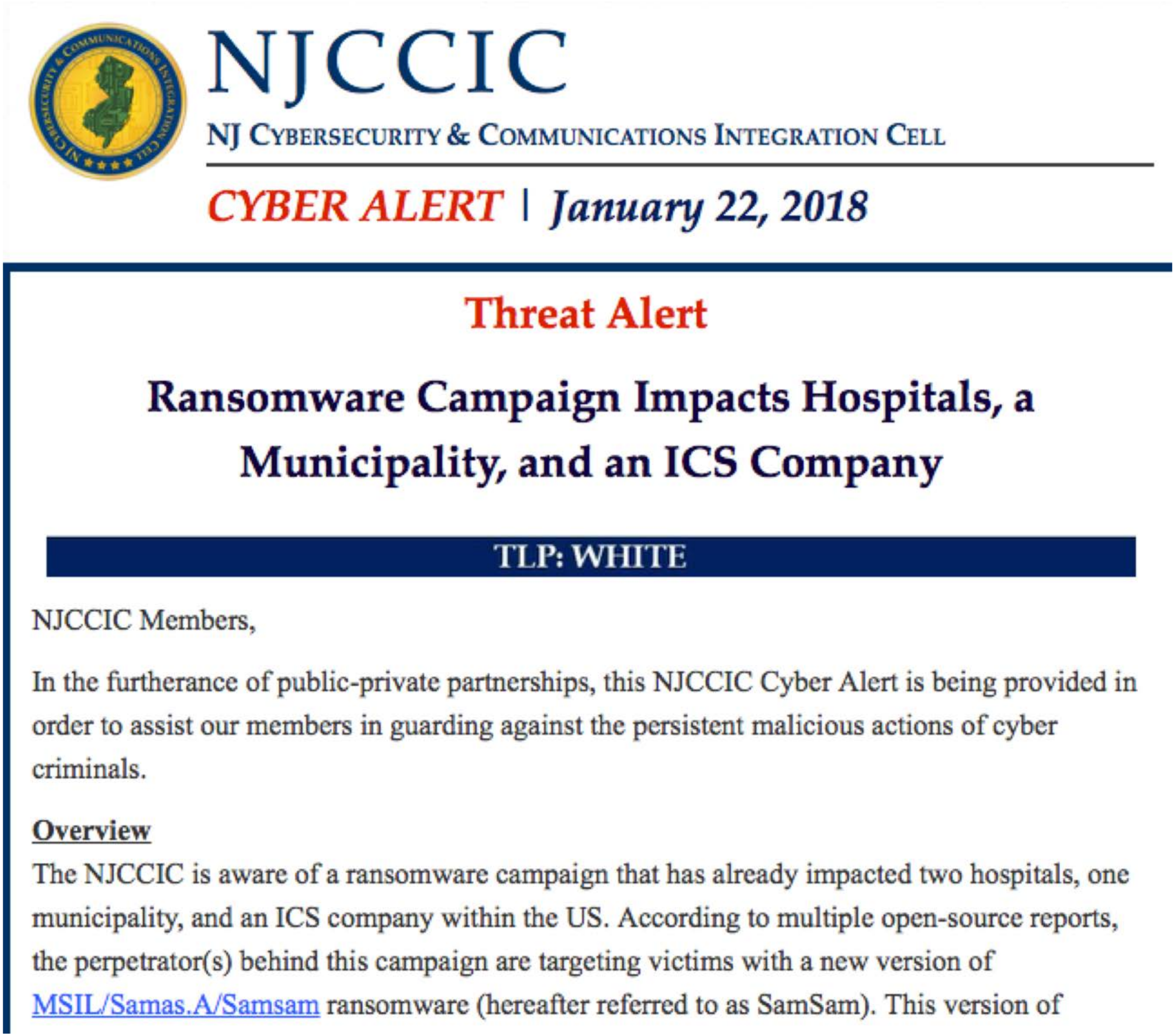
POSSIBLE ACTORS

- Nation-State Actors
- Criminals
- Black Hat Hackers
- Insiders
- Terrorists
- Politically Motivated Groups

POSSIBLE MOTIVATIONS

- Financial Gain
- Retribution for Perceived Grievances
- Fame and Reputation
- Sow Social Division
- Foment Chaos / Anarchy
- Subvert Political Opposition
- Foreign Policy / National Interests
- Undermine Trust in Democracy

Indictments of Iranian Nationals for SamSam Ransomware Attacks



NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

CYBER ALERT | *January 22, 2018*

Threat Alert

Ransomware Campaign Impacts Hospitals, a Municipality, and an ICS Company

TLP: WHITE

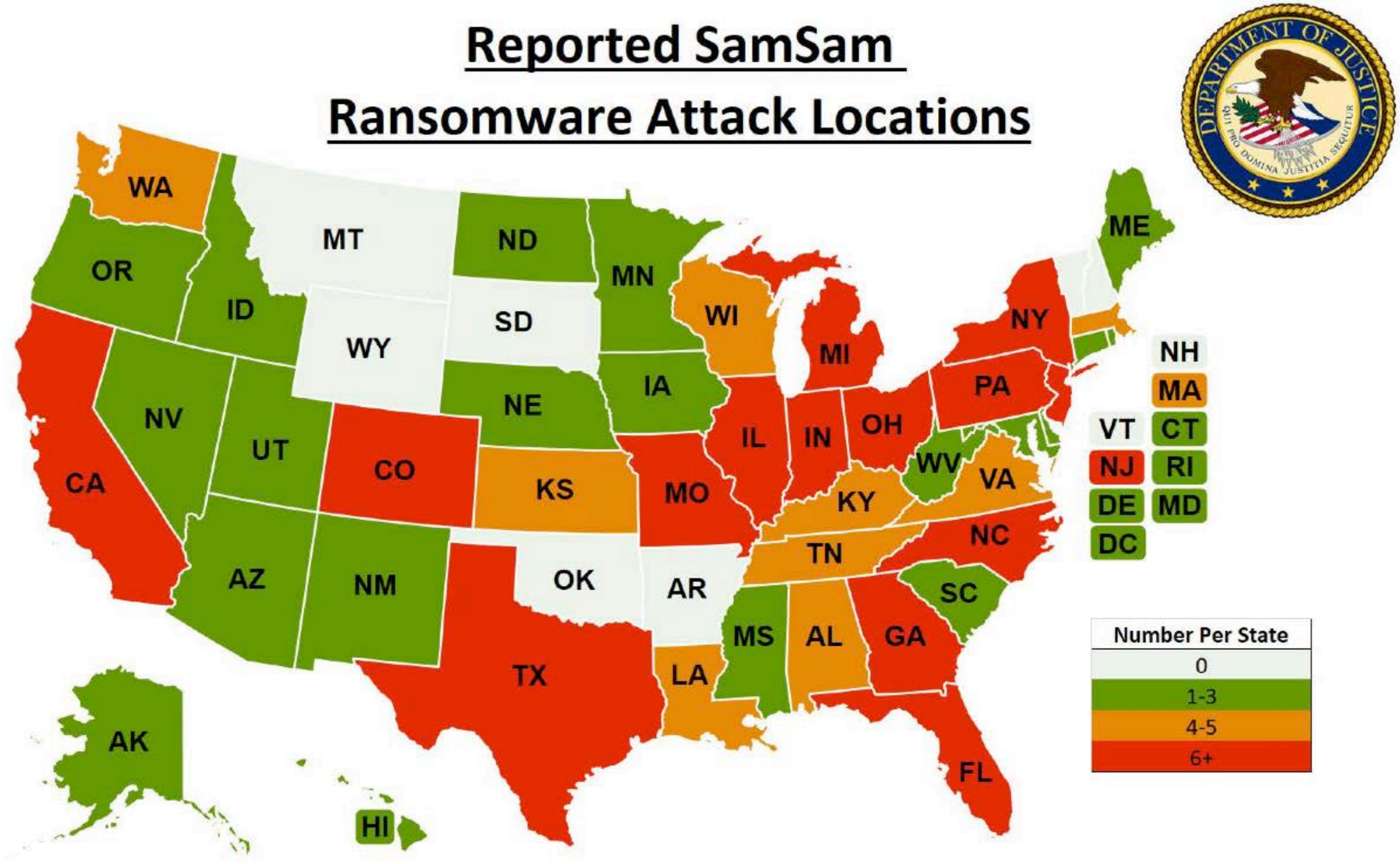
NJCCIC Members,

In the furtherance of public-private partnerships, this NJCCIC Cyber Alert is being provided in order to assist our members in guarding against the persistent malicious actions of cyber criminals.

Overview

The NJCCIC is aware of a ransomware campaign that has already impacted two hospitals, one municipality, and an ICS company within the US. According to multiple open-source reports, the perpetrator(s) behind this campaign are targeting victims with a new version of MSIL/Samas.A/Samsam ransomware (hereafter referred to as SamSam). This version of

Security Ecosystem: Indictments of Iranian Nationals for SamSam Ransomware Attacks



Reported SamSam Ransomware Attack Locations

Indictments of Iranian Nationals for SamSam Ransomware Attacks

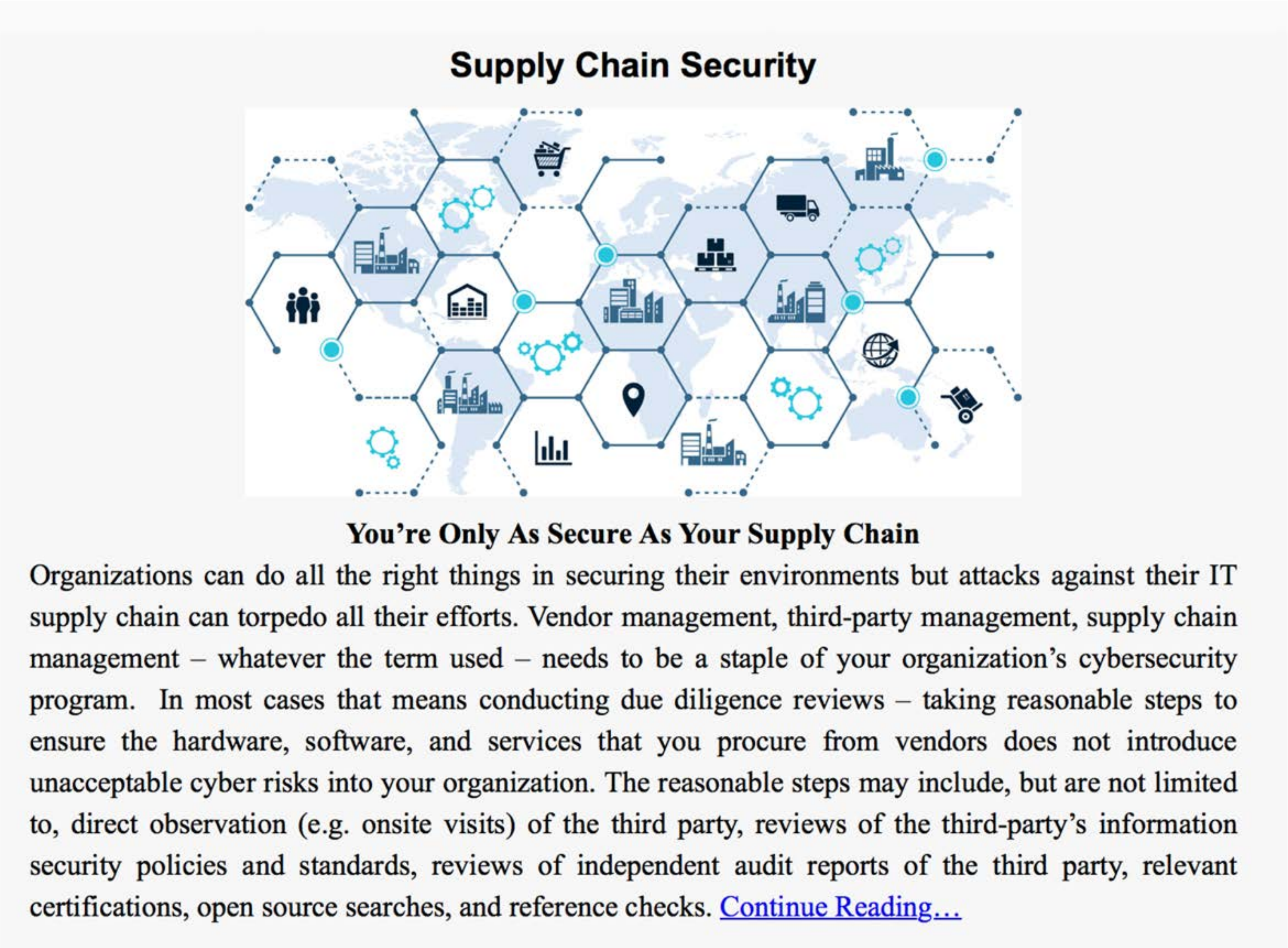
“To execute the SamSam ransomware attack, cyber actors exploit computer network vulnerabilities to gain access and copy the SamSam ransomware into the network. Once in the network, these cyber actors use the SamSam ransomware to gain administrator rights that allow them to take control of a victim’s servers and files, without the victim’s authorization.”

US DOJ

- Hollywood Presbyterian Hospital
- City of Atlanta
- Colorado Department of Transportation
- City of Newark, NJ
- Port of San Diego

- Hollywood Presbyterian Hospital

Willie Sutton Rule



Supply Chain Security

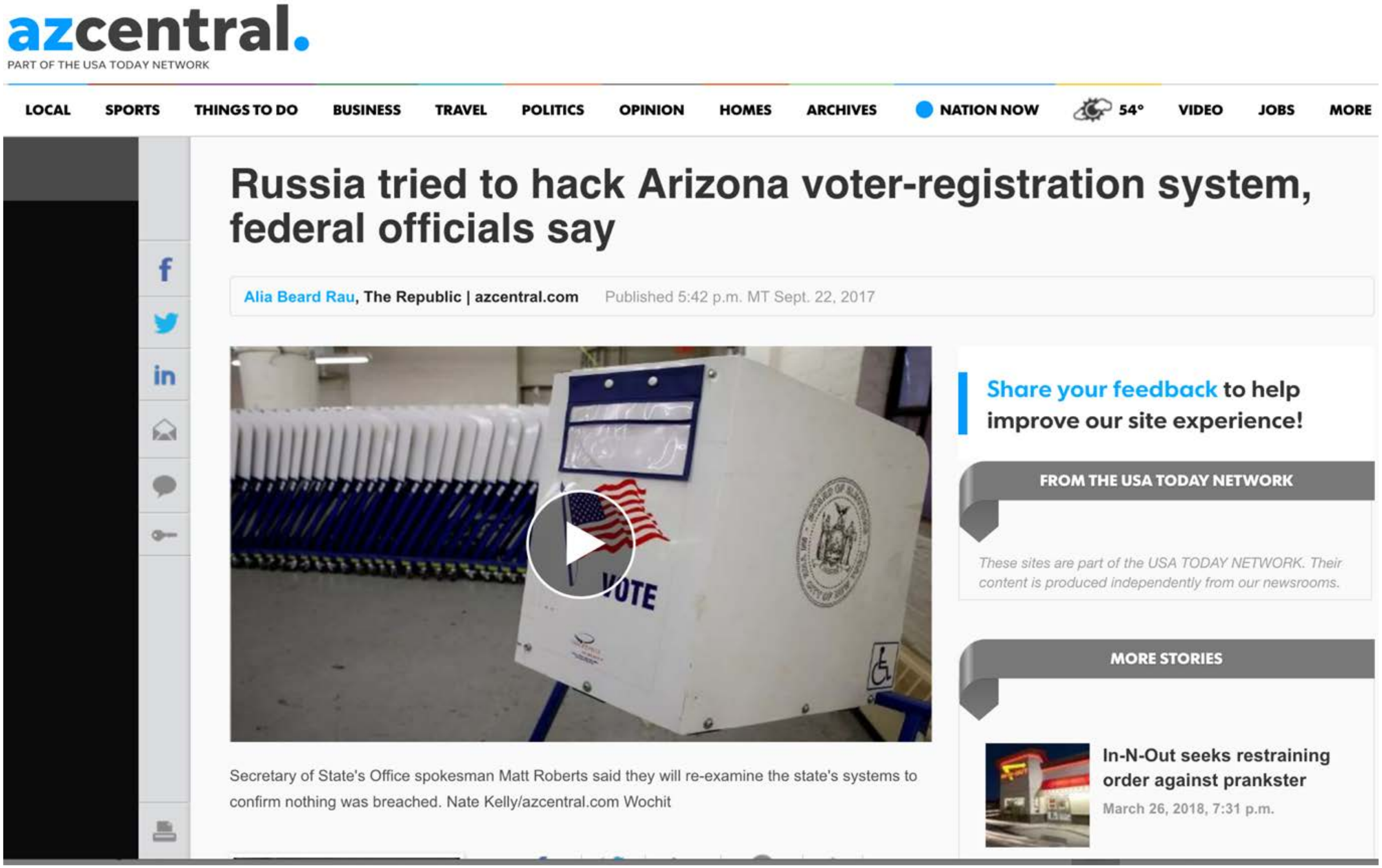
You’re Only As Secure As Your Supply Chain

Organizations can do all the right things in securing their environments but attacks against their IT supply chain can torpedo all their efforts. Vendor management, third-party management, supply chain management – whatever the term used – needs to be a staple of your organization’s cybersecurity program. In most cases that means conducting due diligence reviews – taking reasonable steps to ensure the hardware, software, and services that you procure from vendors does not introduce unacceptable cyber risks into your organization. The reasonable steps may include, but are not limited to, direct observation (e.g. onsite visits) of the third party, reviews of the third-party’s information security policies and standards, reviews of independent audit reports of the third party, relevant certifications, open source searches, and reference checks. Continue Reading…

Credential Compromise

- Credentials are the keys to the kingdom
- Less than 35% of users have unique passwords across sites
- 28% of organizations provide multi-factor authentication (MFA)
- 78% of users within organizations that provide MFA hate it
- Privileged access: “Do as I say, not as I do”

Beyond Account Takeover



Russia tried to hack Arizona voter-registration system, federal officials say

Alia Beard Rau, The Republic | azcentral.com Published 5:42 p.m. MT Sept. 22, 2017

Secretary of State's Office spokesman Matt Roberts said they will re-examine the state's systems to confirm nothing was breached. Nate Kelly/azcentral.com Wochit

Share your feedback to help improve our site experience!

FROM THE USA TODAY NETWORK

These sites are part of the USA TODAY NETWORK. Their content is produced independently from our newsrooms.

MORE STORIES

In-N-Out seeks restraining order against prankster

March 26, 2018, 7:31 p.m.

NJCCIC
New Jersey Cybersecurity & Communications Integration Cell

THE WEEKLY BULLETIN

November 15, 2018

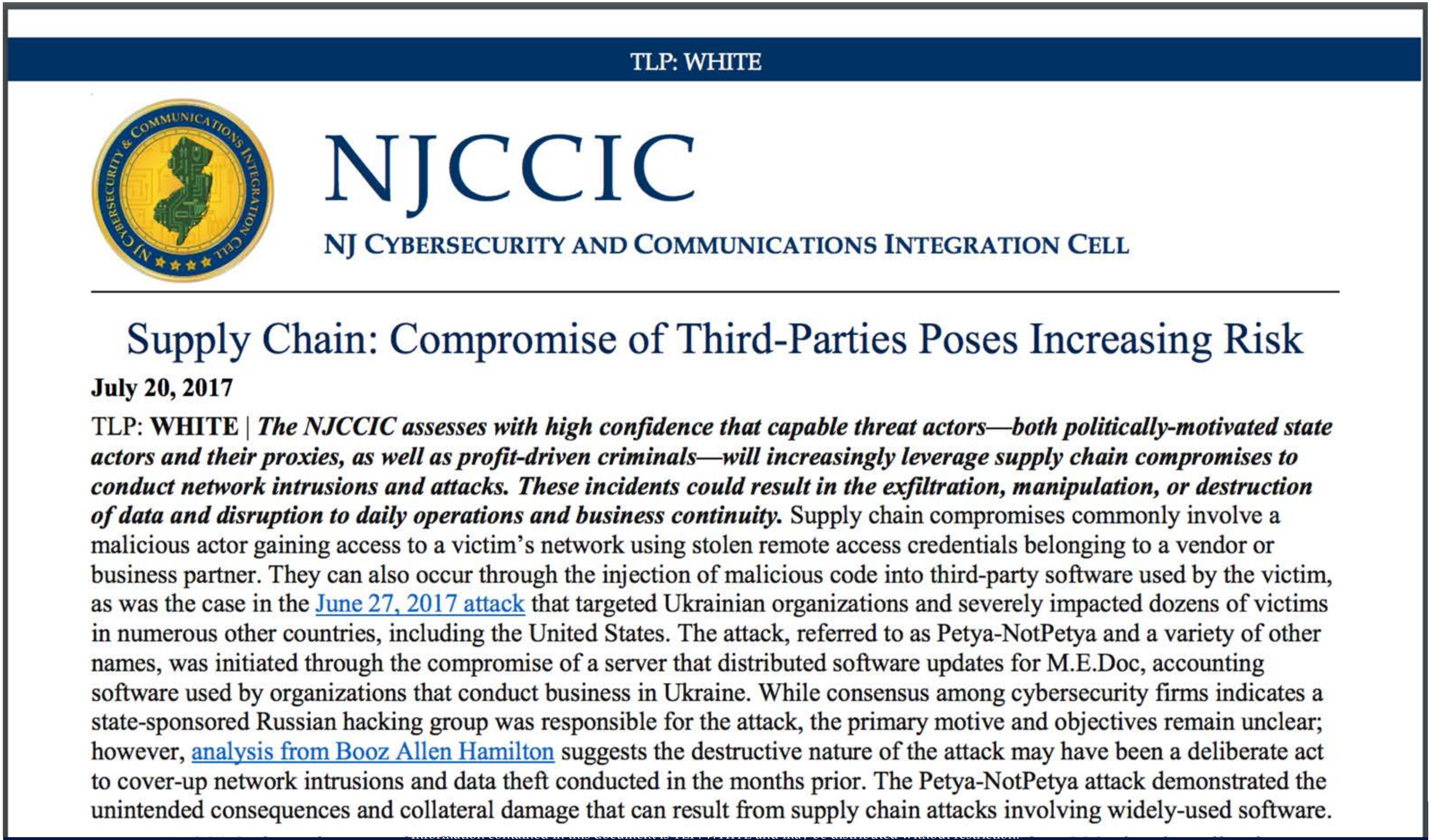
TLP: WHITE

Garden State Cyber Threat Highlight

Providing our members with a weekly insight into the threats and malicious activity directly targeting New Jersey networks.

Emotet Campaigns Persist, Utilize Updated Tactics and Techniques

Supply Chain Security



TLP: WHITE

NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Supply Chain: Compromise of Third-Parties Poses Increasing Risk

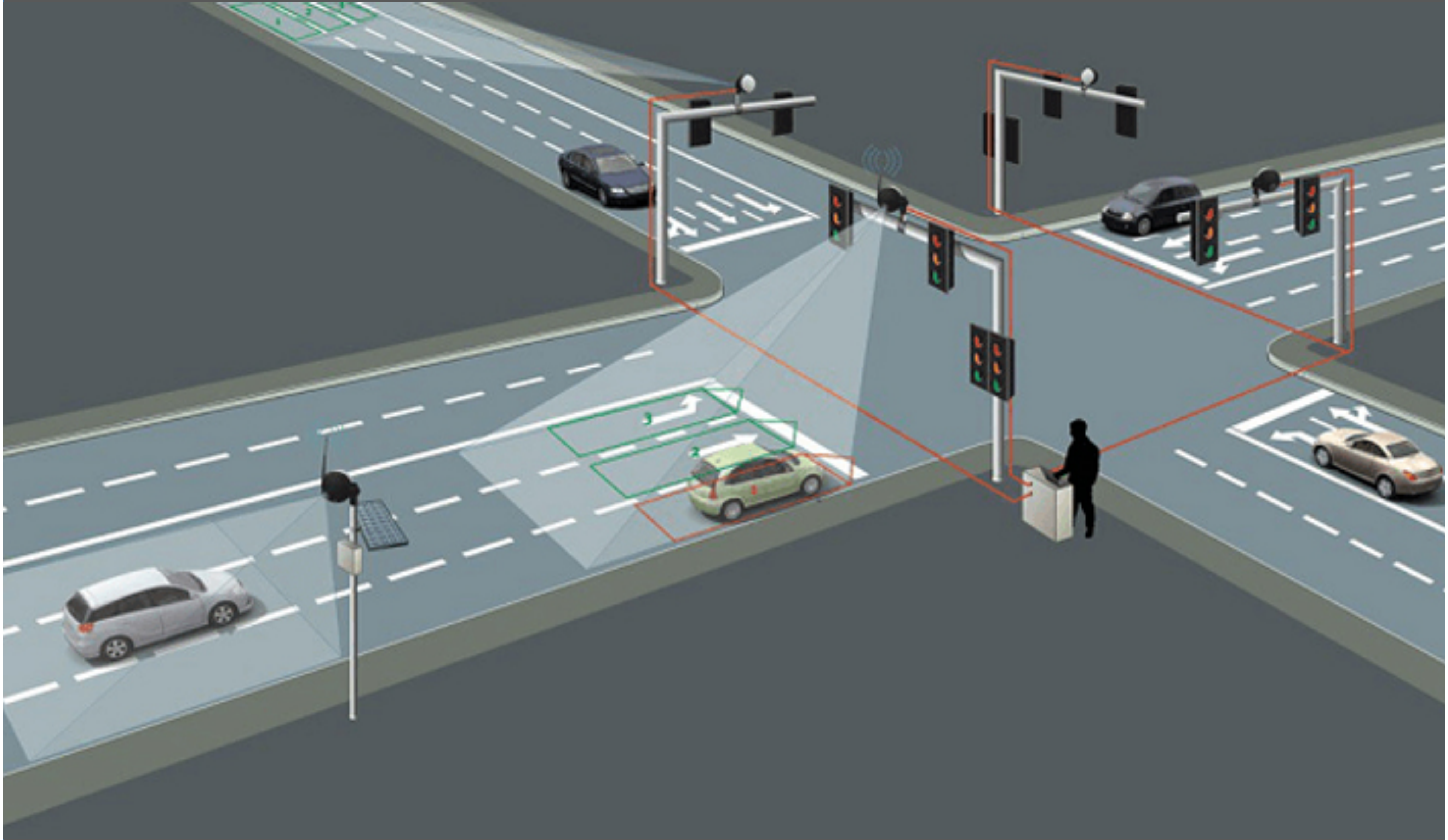
July 20, 2017

TLP: **WHITE** | ***The NJCCIC assesses with high confidence that capable threat actors—both politically-motivated state actors and their proxies, as well as profit-driven criminals—will increasingly leverage supply chain compromises to conduct network intrusions and attacks. These incidents could result in the exfiltration, manipulation, or destruction of data and disruption to daily operations and business continuity.*** Supply chain compromises commonly involve a malicious actor gaining access to a victim's network using stolen remote access credentials belonging to a vendor or business partner. They can also occur through the injection of malicious code into third-party software used by the victim, as was the case in the June 27, 2017 attack that targeted Ukrainian organizations and severely impacted dozens of victims in numerous other countries, including the United States. The attack, referred to as Petya-NotPetya and a variety of other names, was initiated through the compromise of a server that distributed software updates for M.E.Doc, accounting software used by organizations that conduct business in Ukraine. While consensus among cybersecurity firms indicates a state-sponsored Russian hacking group was responsible for the attack, the primary motive and objectives remain unclear; however, analysis from Booz Allen Hamilton suggests the destructive nature of the attack may have been a deliberate act to cover-up network intrusions and data theft conducted in the months prior. The Petya-NotPetya attack demonstrated the unintended consequences and collateral damage that can result from supply chain attacks involving widely-used software.

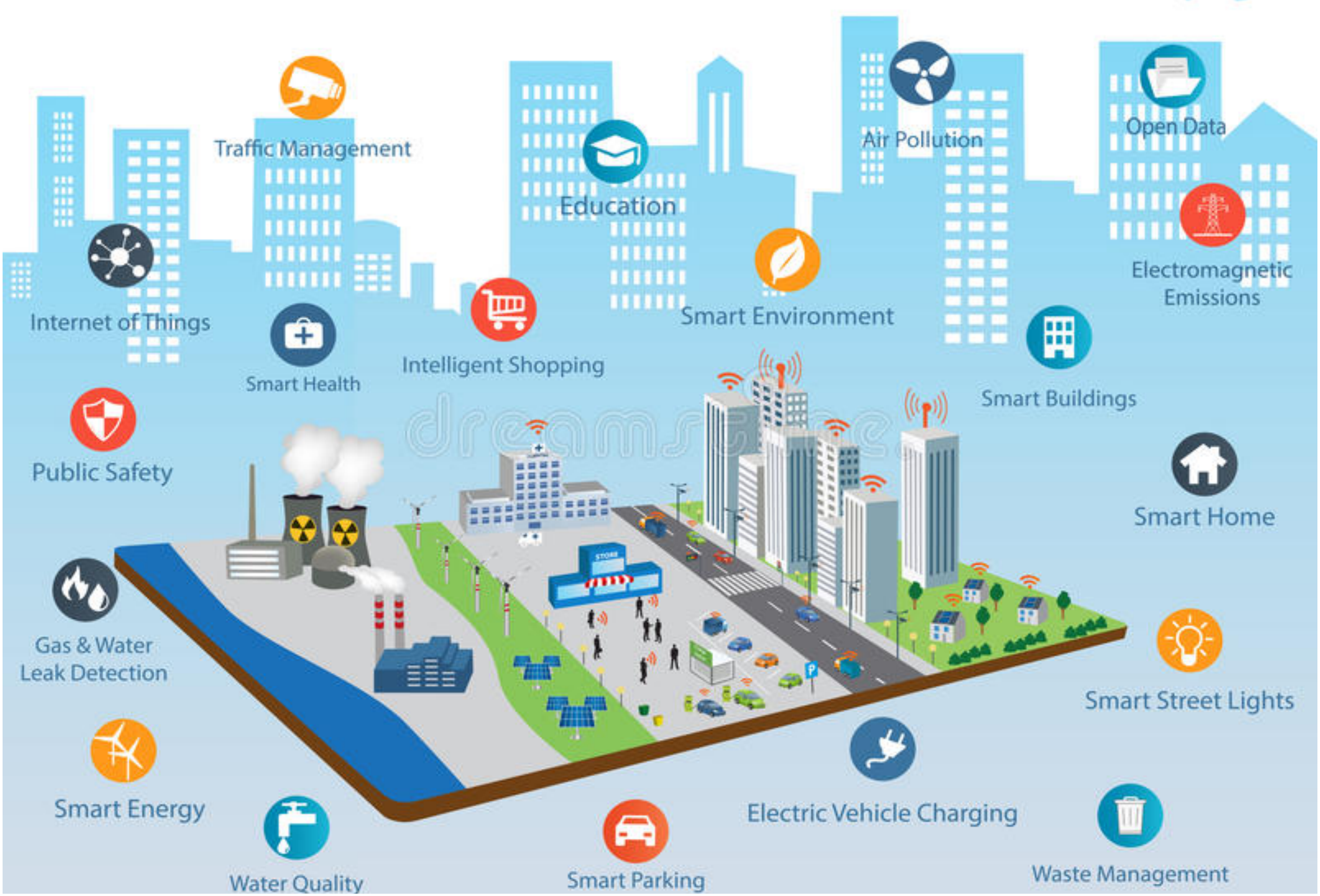
Information contained in this document is TLP: WHITE and may be distributed without restriction.

Convergence

Intelligent Traffic Systems



SMART CITY


Traffic Management
Education
Air Pollution
Open Data
Internet of Things
Smart Environment
Electromagnetic Emissions
Smart Health
Intelligent Shopping
Smart Buildings
Public Safety
Smart Home
Gas & Water Leak Detection
Smart Street Lights
Smart Energy
Electric Vehicle Charging
Water Quality
Smart Parking
Waste Management
STORE
P

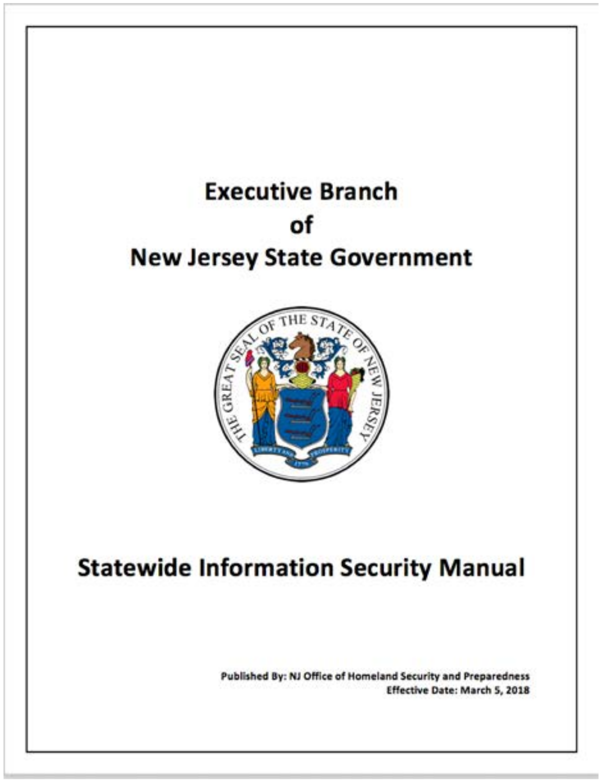
NJCCIC Services

- Threat Intelligence – alerts, advisories, bulletins, threat briefings
- Best Practices
- Incident Response Support
- Training
- NJCCIC Affiliate Program (2019)
- US DHS, MS-ISAC

Best Practices for Managing Risk

NJCCIC Cybersecurity Program Controls Assessment

- Aligned with Statewide Information Security Manual
- Self-Assessment covering 33 Control Areas
- Allows organization and NJCCIC to identify risks and establish strategies and tactics to manage them

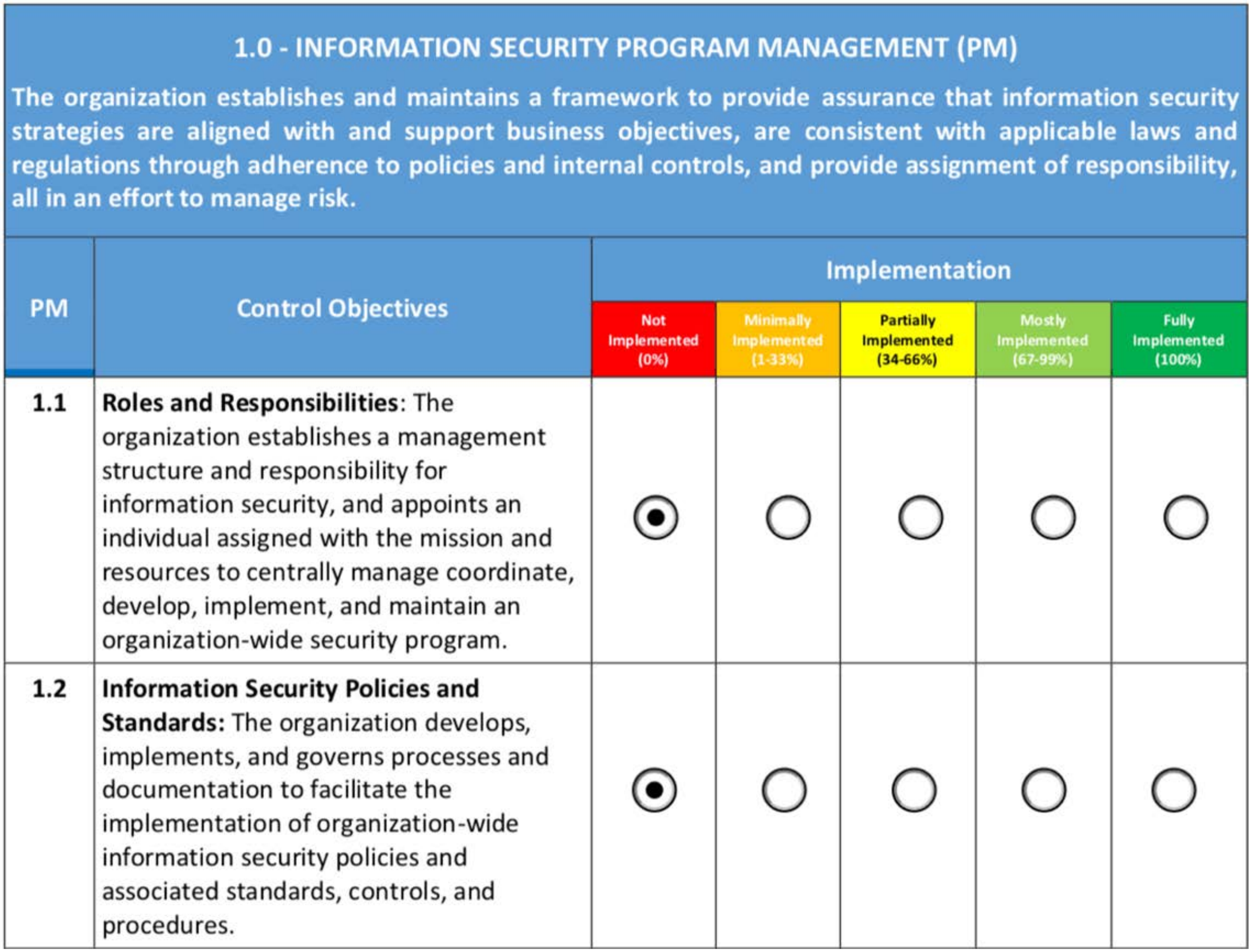


Executive Branch
of
New Jersey State Government

Statewide Information Security Manual

Published By: NJ Office of Homeland Security and Preparedness
Effective Date: March 5, 2018

NJCCIC Cybersecurity Program Controls Assessment

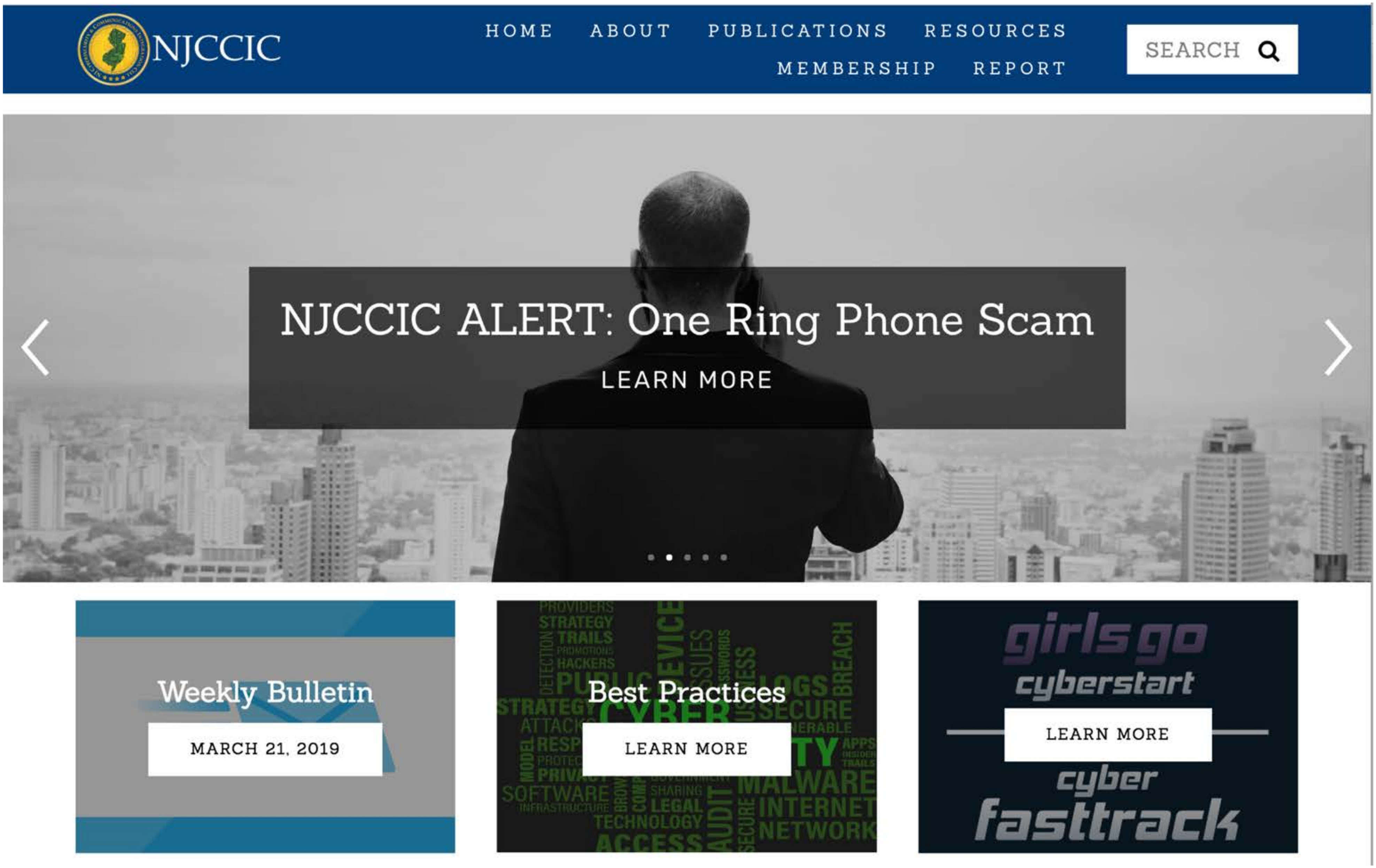


1.0 - INFORMATION SECURITY PROGRAM MANAGEMENT (PM)

The organization establishes and maintains a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

PM	Control Objectives	Implementation				
		Not Implemented (0%)	Minimally Implemented (1-33%)	Partially Implemented (34-66%)	Mostly Implemented (67-99%)	Fully Implemented (100%)
1.1	**Roles and Responsibilities**: The organization establishes a management structure and responsibility for information security, and appoints an individual assigned with the mission and resources to centrally manage coordinate, develop, implement, and maintain an organization-wide security program.	●	○	○	○	○
1.2	**Information Security Policies and Standards:** The organization develops, implements, and governs processes and documentation to facilitate the implementation of organization-wide information security policies and associated standards, controls, and procedures.	●	○	○	○	○

www.cyber.nj.gov



Connect With NJCCIC

NJCCIC@cyber.nj.gov

609-963-6900 x7865

@NJCybersecurity

cyber.nj.gov