Cybersecurity Governance in the State of New Jersey

A CASE STUDY

December 2017

Homeland Security

NASCIO Representing Chief Information Officers of the States

New Jersey State Fast Facts[1,2]

ELECTED OFFICIALS:

- Governor Chris Christie
- New Jersey General Assembly: 80 Members of the Assembly
- New Jersey State Senate: 40 Senators[3]

STATE CYBERSECURITY EXECUTIVES:

- Chief Information Security Officer (CISO) Michael Geraghty
- Chief Technology Officer (CTO) David Weinstein

STATE DEMOGRAPHICS:

- Population: 8,832,406
- Workforce in “computers and math” occupations: 3.6%[4]

EDUCATION:

- Public with a high school diploma: 46.1%
- Public with an advanced degree: 42.1%

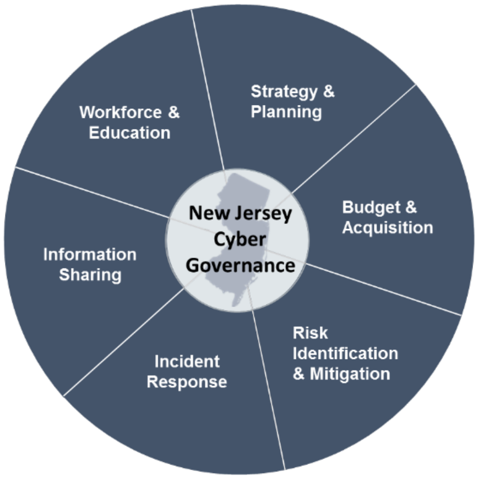
COLLEGES AND UNIVERSITIES:

- 19 community colleges[5]
- 15 private colleges
- 10 public research universities and state colleges[6]

KEY INDUSTRIES:[7]

- Agriculture
- Finance
- Healthcare
- Life sciences
- Logistics
- Manufacturing
- Technology

Executive Summary



The Overall Challenge:

How to address a range of cybersecurity challenges that cut across multiple government, public, and private sector organizations?

Overall Lessons Learned from New Jersey's Governance Approach:

- **Leadership Matters**. Leaders across multiple government, public, and private organizations make cybersecurity, and cybersecurity governance, a priority.
- **Leadership Is Not Everything**. Laws, policies, structures, and processes instantiate and align cybersecurity governance with cybersecurity priorities so that focus does not change as personalities change.
- **Governance Crosses Organizational Boundaries.** The distributed nature of cybersecurity requires a range of governance mechanisms that connect across multiple organizations and sectors.

This case study describes how New Jersey has used laws, policies, structures, and processes to help govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. It explores cross-enterprise governance mechanisms used by New Jersey across a range of common cybersecurity areas—strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, and workforce and education.*

This case study is part of a pilot project intended to demonstrate how states use governance mechanisms to help prioritize, plan, and make cross-enterprise decisions about cybersecurity. It offers concepts and approaches to other states and organizations that face similar challenges. As the case covers a broad range of areas, each related section provides an overview of New Jersey's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with New Jersey to better understand how to tailor solutions to their specific circumstances.

A law passed in 2007 helped lay the foundation for New Jersey's current cybersecurity initiatives by consolidating information technology (IT) services from across executive branch agencies into one agency—the Office of Information Technology (OIT).[8] This change allowed the state to coordinate IT "planning, budgeting, and spending throughout the Executive Branch to advance cost savings, improve the quality of services, and retain operating efficiencies."[9] (In

* For purposes of this case study, governance refers to the laws, policies, structures, and processes that enable people within and across organizations to address challenges in a coordinated manner through activities such as prioritization, planning, and decision making.

this case study, “agency” refers to executive branch agencies.) This, in turn, provided a foundation for executive leaders to launch a series of deliberate steps beginning in 2015 to strengthen cross-organizational cybersecurity governance. This case, therefore, will focus primarily on changes made since approximately 2015 and recognizes that the state is still in the process of developing and implementing its cross-ecosystem cybersecurity governance.

In 2015, Governor Chris Christie signed an executive order establishing the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC), a central civilian body designed to “coordinate cybersecurity information sharing, perform cybersecurity threat analysis, and promote shared and situational awareness between and among the public and private sectors.”[10]

The NJCCIC is part of the New Jersey Office of Homeland Security and Preparedness (OHSP), a reflection of the state’s view of cyber as a security issue rather than strictly an IT issue.[11] As state Chief Information Security Officer (CISO) Mike Geraghty said, “By moving the CISO under the homeland security function within the state, risks are reported within an environment with a lot of the right assets in place, such as state police, intelligence analysts and information sharing resources.”[12]

The Director of OHSP is responsible for “the strategic development, execution, and management of an effective and efficient information security program to manage cyber risks and ensure the confidentiality, integrity, and availability of the Executive Branch’s information assets.”[13] The CISO, who reports to the Director of OHSP, serves as the head of the OHSP Division of Cybersecurity and leads the state’s cybersecurity strategic planning, information sharing, and incident response efforts.[14]

The CISO collaborates with the Chief Technology Officer (CTO), who leads OIT and issues policies designed to protect the state’s assets and networks, and ensures that state departments and agencies follow the CISO and CTO policies. [15] The CTO, who is a member of the cabinet and reports directly to the Governor, is responsible for supporting the state information security program. This is accomplished by designing, acquiring, and implementing an enterprise IT system—in compliance with information security policies and standards set by the state CISO—and operating the IT systems in compliance with CISO-approved security procedures, such as malware protection, data encryption, and software patch management. As part of this responsibility, the CTO ensures that policies are implemented by the individual departments and agencies.

In 2017, OIT and NJCCIC leaders collaborated and issued a series of new information security policies to provide foundational direction to state departments and agencies. Among the first policies to be drafted and issued were the state’s cyber incident response policy and plan; cybersecurity organizational roles and responsibilities; and state department and agency IT acquisition policy.

In addition to the priorities outlined above, New Jersey has developed information sharing structures and mechanisms to disseminate threat information with the government and private sector. For example, the NJCCIC shares information with more than 39 states, 42 federal agencies, state executive departments and agencies, local governments, 13 international countries (such as the UK, Australia, and Germany), and many companies. Also, reflective of the importance of the financial industry to the economy, the NJCCIC formed a partnership with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to share and analyze cyber threats to the financial industry. In addition, there are two formal information sharing bodies—the Domestic Security Preparedness Task Force (DSPTF) and the Infrastructure Advisory Committee (IAC)—that include private sector membership. The DSPTF and IAC raise cybersecurity issues facing private industry to the attention of executive branch leaders.

New Jersey demonstrates cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders. Therefore, New Jersey uses a range of governance mechanisms to work across organizations. As New Jersey is in the process of strengthening and expanding cross-ecosystem cybersecurity governance, much of the initial focus has been on strengthening cross-government cybersecurity, filling some of the most important cybersecurity roles in the state, such as the CTO, CISO and Director of OHSP, and building on New Jersey's public/private information sharing mechanisms.

Table of Contents

Background & Methodology

This case study was developed as part of a pilot project to identify how states have used laws, policies, structures, and processes to help better govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. This project emerged as a result of the *Department of Homeland Security (DHS) Advisory Council Final Report of the Cybersecurity Subcommittee, Part II – State, Local, Tribal & Territorial (SLTT*), which recognized the importance of governance in addressing a range of cybersecurity technology and operational challenges.[16]

The case study explores cross-enterprise governance mechanisms used by New Jersey across a range of common cybersecurity areas—strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, and workforce and education. It is not intended to serve as a formal evaluation. Instead, the case offers concepts and approaches that may be useful to other states and organizations that face similar challenges. As this case covers a broad range of areas, each related section provides an overview of New Jersey's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with New Jersey to better understand how to tailor solutions to their specific circumstances.

DHS' Office of Cybersecurity and Communications (CS&C) initiated and leads the project in partnership with the National Association of State Chief Information Officers (NASCIO). NASCIO is a nonprofit association "representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia."[17] The Homeland Security Systems Engineering and Development Institute (HSSEDI), a DHS owned Federally Funded Research and Development Center (FFRDC), developed the case studies.

Candidate states were identified to participate in the pilot project based on:

- analysis of third party sources,
- diversity of geographic region, and
- recommendations from DHS and NASCIO with awareness of SLTT cybersecurity practices.

Candidate states that agreed to participate in the DHS-led pilot project did so on a voluntary basis. Researchers used open source material and conducted a series of interviews to gather the necessary information to develop each state case study.

I. Strategy & Planning

Strategy & Planning
Budget & Acquisition
Risk Identification & Mitigation
Incident Response
Information Sharing
Workforce & Education

The Challenge:

How to set direction and prioritize cybersecurity initiatives across multiple organizations?

Features of New Jersey's Governance Approach:

- The CISO is charged with developing a statewide cybersecurity strategy.
- A cross-enterprise information security program is operationalized via policies and standards developed by the OHSP and OIT.
- An intra-governmental committee brings a cross-organizational perspective to the development of state cybersecurity strategy.

The CISO, who was hired in 2016 and reports to the Director of the OHSP (see Figure 1 below), is charged with developing a statewide cybersecurity strategy. This responsibility is part of the CISO's overall mission to establish and manage "an information security program to ensure the confidentiality, integrity, and availability" of the executive branch's "information resources, systems, and services while promoting and protecting privacy" and "developing, implementing and monitoring the performance of the information security program."[18] The CISO:

- Sets strategic information security plans across the executive branch,
- Publishes and maintains the statewide Information Security Policies and Standards,
- Develops, maintains, and interprets the Information Security Policies and Standards, and
- Provides cybersecurity subject matter expertise to state agencies.[19]

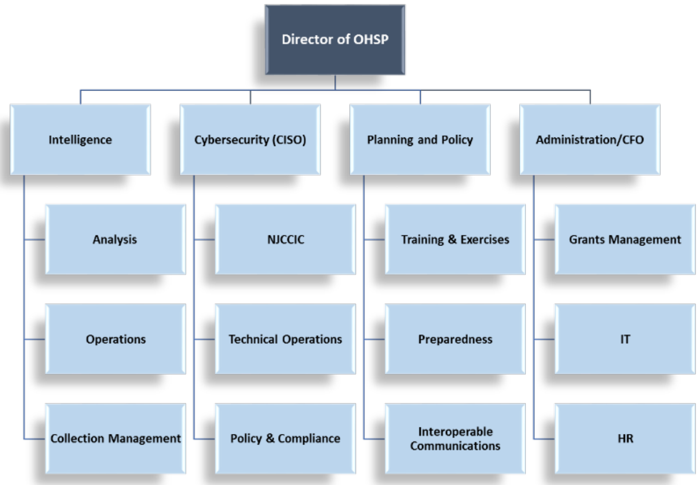


Figure 1. New Jersey Office of Homeland Security and Preparedness[20]

When this case was being developed, the CISO was in the final stages of completing a formal cybersecurity strategic plan guided by several government and industry-authored frameworks.[21] However, the Director of OHSP, the CTO, and CISO shared a common strategic perspective about the need for a cross-enterprise information security program. They have taken several steps in the last year to instantiate this program via policies and standards that address cyber risk identification and mitigation, cyber incident response, and information sharing (see Section II, Budget & Acquisition; Section III, Risk Identification & Mitigation; and Section V, Information Sharing).[22]

To bring a cross-organizational perspective to the development of state cybersecurity strategy, in January 2017 OIT policy created the Information Security Governance Committee (ISGC), an intra-governmental body co-chaired by the Director of the OHSP and the CTO. The ISGC, which is in the process of being stood up, is intended to play a strategic role in cybersecurity issues within the state and reports to the cabinet. ISGC members include the state CISO, the state Chief Data Officer (CDO), representatives from the Department of Treasury, and other state agencies as appropriate.[23] The ISGC is responsible for:[24]

- Assisting the CISO in overseeing and executing the state's information security management program,
- Reviewing the Enterprise Information Security Policies and Standards—and subsequent amendments—to ensure their alignment with the executive branch business objectives and goals, risk tolerances, and statutory, regulatory, and contractual requirements,
- Providing direction and counsel regarding the assessment and management of information security risks and cyber threats to the state of New Jersey,
- Reviewing reports on major information security incidents and cases of noncompliance,
- Overseeing the response to information security incidents,
- Reviewing security metrics and trends regarding the overall performance of the information security program, and
- Staying abreast of cybersecurity threats to the executive branch of state government through briefings and reports.

II. Budget & Acquisition

Strategy & Planning
Workforce & Education
Budget & Acquisition
Information Sharing
Risk Identification & Mitigation
Incident Response

The Challenge:

How to manage investments in strategic cybersecurity priorities as part of budget and acquisition processes across multiple organizations?

Features of New Jersey's Governance Approach:

- Agencies use annual IT budget to reimburse OHSP and/or OIT for some enterprise-wide cyber-related services.
- Acquisition policy is designed to reduce cyber risks by centralizing authorization for certain services and products with the CTO.

The OHSP and OIT use a variety of budget and acquisition governance mechanisms to drive and influence cybersecurity practices throughout state departments and agencies.

While each agency receives an annual IT budget, some of this budget is used to reimburse OHSP and OIT for enterprise-wide cyber-related services. Reimbursement levels are set according to agency headcount or workstation count, with the larger organizations paying more than smaller organizations. For example, OIT provides a vendor solution called "Websense" to all executive agencies to help filter internet content available to users on the state's network.[25] Access to certain sites is restricted in keeping with the state's internet user agreement and risk profile, and Websense provides a mechanism to operationalize this policy. The OIT purchased a global license to Websense and charges agencies a fee based on usage to cover the cost of the license.[26] Websense is one of many information security tools the CTO uses to ensure user safety on the state's network. NJCCIC also provides some enterprise-wide cybersecurity protections, such as next generation firewalls, intrusion prevention systems, and a security information and event management system.[27]

In addition to budget, New Jersey uses acquisition policy to drive cybersecurity. In September 2017, a new procurement policy established procedures that apply to department and agency acquisition of IT hardware, software, and subscription-based services. The purpose of the policy is, in part, to reduce the risk of cybersecurity threats to the state's network by centralizing IT acquisition with the OIT CTO to ensure that any new technology or service introduced into the state's network receives proper vetting to comply with information security standards set by the CISO.

The policy expressly prohibits agencies from purchasing "any information technology infrastructure, regardless of dollar value, unless granted approval due to exceptional circumstances by OIT."[28] IT infrastructure is defined as "computing, storage, network and data center assets (e.g. servers, routers, racks)."[29] In addition, the new policy requires

CTO approval for upgrades to IT infrastructure that may impact information security.[30]

The OIT CTO reviews and approves IT purchases exceeding $50,000, while those exceeding $100,000 must undergo OIT and Office of Management and Budget (OMB) review and approval.[31]

III. Risk Identification & Mitigation

Strategy & Planning
Budget & Acquisition
Risk Identification & Mitigation
Incident Response
Information Sharing
Workforce & Education

The Challenge:

How to identify and mitigate cybersecurity risks across multiple organizations?

Features of New Jersey's Governance Approach:

- Cybersecurity risk identification and mitigation activities are a shared responsibility between the CISO, CTO, and state agencies.
- The CISO and CTO are primarily responsible for policy setting and review, while agencies are primarily responsible for implementation.
- The CTO uses a Systems Architecture Review (SAR) process to ensure agency systems and services comply with the CISO's guidelines.
- The CTO also has execution responsibilities, including the day-to-day security management of enterprise information, systems, and solutions.

The state's cybersecurity risk identification and mitigation activities are a shared responsibility between the CISO, CTO, and state departments and agencies. The CISO and CTO are primarily responsible for policy setting and review, while agencies are primarily responsible for implementation.

The CISO establishes the overarching requirements, standards, and metrics for cybersecurity in departments and agencies. Based on 2017 policy, the CISO is responsible for:[32]

- Identifying security requirements to limit risks associated with executive business objectives, and
- Providing security metrics to track the performance of the information security program.

The CISO is also responsible for developing an Information Security Governance, Risk, and Compliance program, including, but not limited to:

- Coordinating and conducting compliance and risk assessments of agencies and their information assets,
- Conducting and managing vulnerability assessments of agency networks, applications, databases, and systems,

- Conducting penetration tests of agency networks, applications, databases, and systems, and
- Conducting information security risk assessments of third parties with access to state of New Jersey information assets.

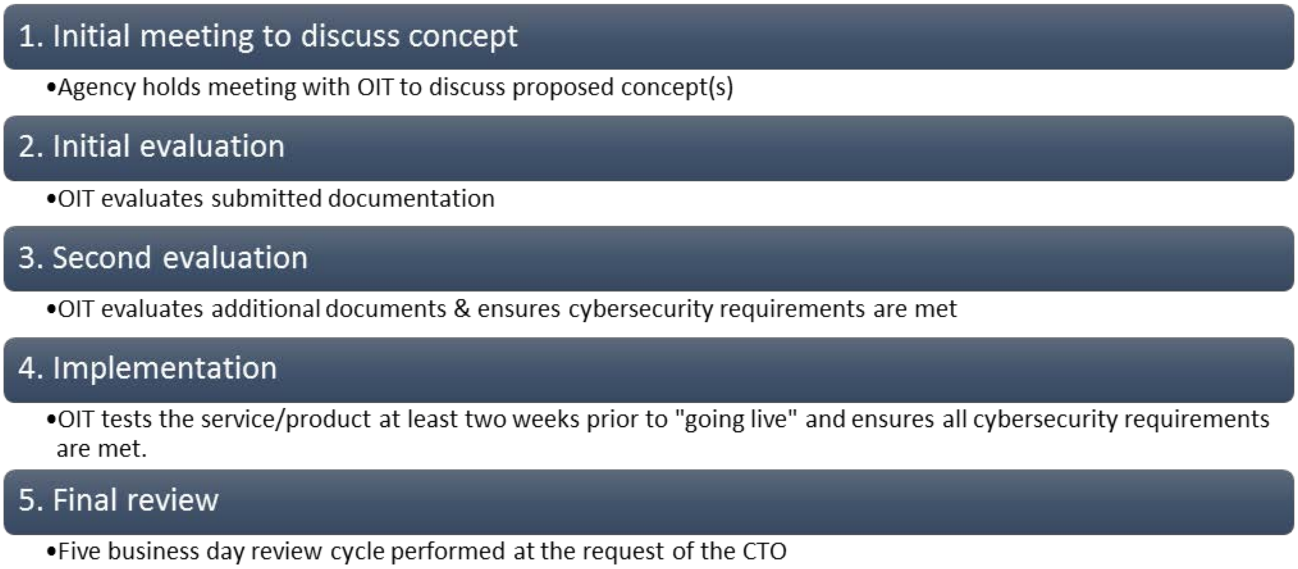
The program, for example, is on track to conduct 50 risk assessments, 1,500 system vulnerability assessments, and 1,500 application vulnerability assessments in FY2018.[33]

As described above in Section I, Strategy & Planning, the ISGC, which is co-chaired by the Director of OHSP and the CTO, is in the process of being stood up. It is intended to help the CISO identify potential risks. The ISGC reports to the cabinet and can assist the CISO by reviewing reports of major information security incidents and cases of noncompliance, staying abreast of cybersecurity threats to the executive branch, and providing “direction and counsel regarding the assessment and management of information security risks and cyber threats to the State of New Jersey.”[34]

The CTO is responsible for reviewing “all plans for any modification and/or new installation to Executive Branch information systems,” including hardware, software, and IT architecture “to ensure those modifications are in alignment with the State’s [IT] strategy and in compliance with enterprise architecture standards.”[35] The CTO uses a SAR process to ensure that department and agency systems and services comply with the CISO’s guidelines (see Figure 2).

The SAR includes representation from across the executive branch: the CTO, the department/agency Chief Information Officer (CIO), the OHSP, and the CDO. The purpose of the SAR is to ensure compliance with NJCCIC cybersecurity and IT architecture standards and ensure that a vulnerability and/or risk assessment is performed. The results from the assessment as well as other data collected during the review inform: (1) New Jersey cybersecurity and privacy requirements; (2) potential impacts on existing technology infrastructure and operations; (3) prioritization of resources; and (4) disaster recovery and business continuity requirements.[36]

To identify potential risks, the SAR process entails five steps:



1. Initial meeting to discuss concept

•Agency holds meeting with OIT to discuss proposed concept(s)

2. Initial evaluation

•OIT evaluates submitted documentation

3. Second evaluation

•OIT evaluates additional documents & ensures cybersecurity requirements are met

4. Implementation

•OIT tests the service/product at least two weeks prior to "going live" and ensures all cybersecurity requirements are met.

5. Final review

•Five business day review cycle performed at the request of the CTO

Figure 2. OIT SAR Process[37]

The CTO also has execution responsibilities, including the day-to-day security management of enterprise information, systems, and solutions. For example, an Executive Order signed in June 2017 authorizes the CTO to identify and consolidate state IT assets, such as servers and data centers, and modernize the "hundreds of legacy applications," in part to ensure information security across the enterprise.[38]

To ensure coordination between the CISO and CTO, which has its own risk management responsibilities, the OHSP's Division of Cybersecurity's Governance, Risk and Compliance Bureau (GRCB) meets twice a week with OIT to review all proposed new technology products and services. The GRCB reviews potential risks to ensure that cybersecurity standards are met. An assessment is performed to ensure that a product or service can be integrated into the network without introducing vulnerabilities into the enterprise architecture. The GRCB also ensures that adequate funds are identified within OIT, OHSP, and/or the requesting department or agency.

Agencies are responsible for implementing CISO and OIT policies and "protecting and maintaining the confidentiality, integrity, and availability of information assets" within the department or agency.[39] Agency CIOs also manage third-party vendors under contract to provide information services to the department or agency.[40] Departments/agencies must:[41]

- Identify security requirements to limit cyber risks associated with the agency's business goals and objectives,
- Implement and promote information security awareness within their respective agency,
- Ensure compliance with the CISO-created policies and standards such as:
  - Coordination of risk assessments and compliance audits with the NJCCIC
  - Coordination of vulnerability assessments of agency networks, applications, databases, and systems
  - Coordination of risk assessments of third parties having access to agency information assets
- Assist in the implementation of the Cybersecurity Incident Response Plan, and
- Report all information security incidents to the NJCCIC.

IV. Incident Response

The Challenge:

How to prepare for and respond to cyber incidents that require coordinated action across multiple organizations?

Features of New Jersey's Governance Approach:

- The CISO is responsible for establishing the state's overall cyber incident response policy and plan.
- Agencies are responsible for implementing the plan.
- Policy directs agency heads to form in-house Cybersecurity Incident Response Teams (CSIRTs), which are responsible for incident response.

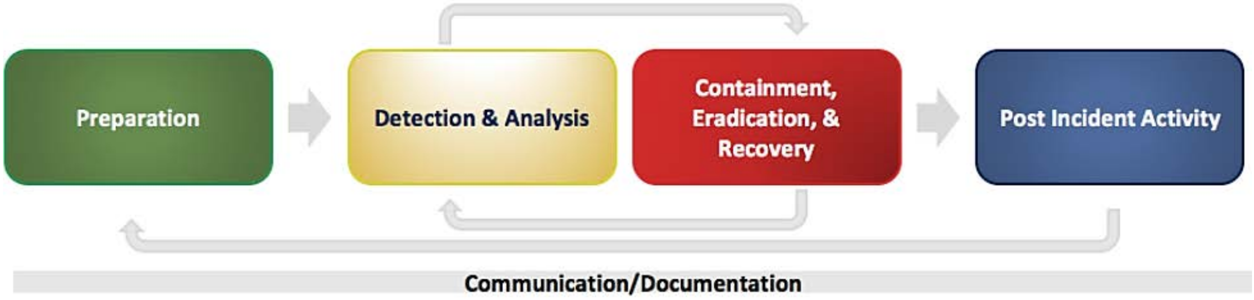
The CISO is responsible for establishing the state's overall cyber incident response policy and plan, while departments and agencies are responsible for implementing the plan. The Director of OHSP is responsible for "overseeing the response to information security incidents."[42]

In 2017, Michael Geraghty, Director of the NJCCIC and the state CISO, rewrote the state's cyber incident response policy and plan. The policy applies to all executive branch agencies, contractors, and third-party vendors, and all "cybersecurity incidents that affect the confidentiality, integrity and availability of agency networks, systems, applications, databases, data and other information assets owned or controlled by the agencies or maintained on their behalf."[43]

The policy describes cyber incident reporting scope, authorities, communication, training, enforcement, and compliance. The cyber response plan ("the plan") describes the roles and responsibilities of incident response team participants, an approach to characterize the incidents, and reporting requirements, and contains sample communications and notification guidance and documentation.[44] Department and agency leaders are responsible for implementing the plan within their respective organizations.[45] The plan, which applies to all executive departments, agencies, commissions, boards, and bodies, focuses on preparation and response to cyber threats that could impact state assets, such as the state network. In the future, the plan is expected to expand and contemplate incidents emanating from external sources, such as private owners/operators of critical infrastructure, that could impact state assets, and/or large-scale incidents that could simultaneously impact multiple state departments and agencies.

The plan incorporates a Cybersecurity Incident Lifecycle ("Lifecycle") and a Cybersecurity Incident Framework ("Framework") (see Figure 3 below).[46] A cybersecurity incident is defined as "any adverse event or condition that has the potential to impact the confidentiality, integrity, and availability of agency information assets."[47]

"The Lifecycle [which consists of four phases] characterizes the continuous efforts agencies makes to handle incidents, while at the same time ensuring continuous improvements in the overall security posture of the Executive Branch of State Government or an agency thereof."[48]



Preparation
Detection & Analysis
Containment, Eradication, & Recovery
Post Incident Activity
Communication/Documentation

Phase	Description
Preparation	Includes activities that enable agencies to respond to an incident, such as development and implementation of policies and procedures, security technologies and tools, training, governance, and communication plans.
Detection & Analysis	Includes the identification and investigation of an incident. During the detection and analysis phase, the incident receives an initial categorization and prioritization. An investigation into the incident with corresponding activities, including evidence collection, documentation of the incident response activities, etc., is initiated during this phase.
Containment, Eradication, & Recovery	Includes all activities involved in the containment of the incident, the eradication of its cause, the restoration of the impacted information assets and the return to normal operations. This phase also involves determining the root cause of the incident.
Post Incident Activity	Includes developing the incident report and disseminating it to appropriate stakeholders; identifying lessons learned from the incident handling process, including the successful and unsuccessful actions taken by an agency in response to the incident; and developing recommendations to prevent future incidents and to improve enterprise security implementation.

Figure 3. New Jersey Cybersecurity Incident Lifecycle

The Framework "consists of a collection of practices and tools that provide agencies with the ability to categorize, prioritize, communicate, track and document incident response activities."[49]

Agencies play a central role in implementing the policy and plan. For example, the incident response policy directs agency heads to form in-house CSIRTs, which are responsible for coordinating and carrying out the agency's response to incidents.[50] CSIRTs are generally comprised of members from the agency: IT team, information security office (ISO), legal, public information office, human resources department, and auxiliary agencies, as necessary (see Figure 4 below). CSIRT members are responsible for carrying out the agency's response to information security incidents, including classifying the incident (by severity, type, etc.). Agency leaders must designate an individual with responsibility to act as the CSIRT Coordinator (typically the agency CIO or ISO). The NJCCIC and OIT support the CSIRTs as necessary to effectively respond to an incident.

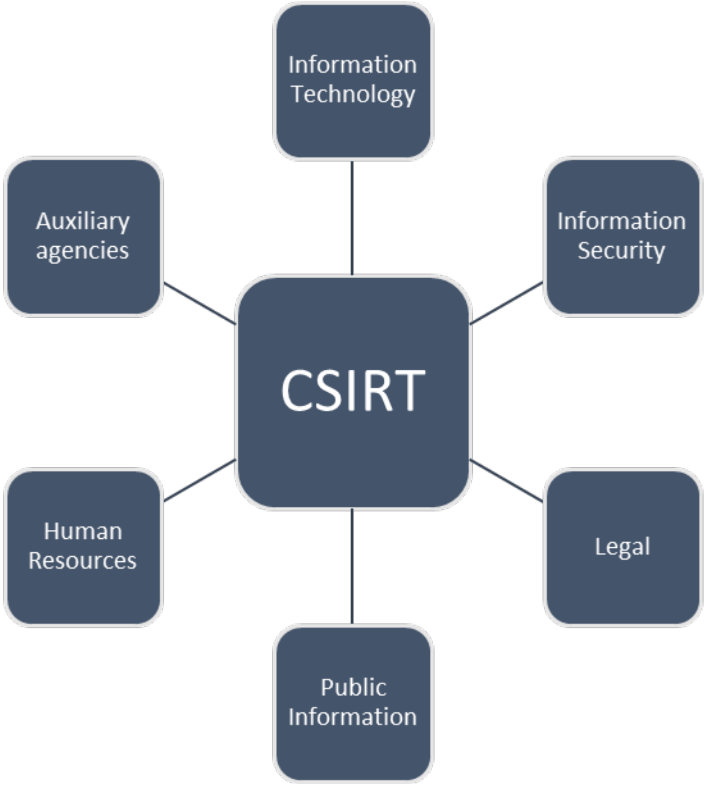


Figure 4. Agency CSIRT

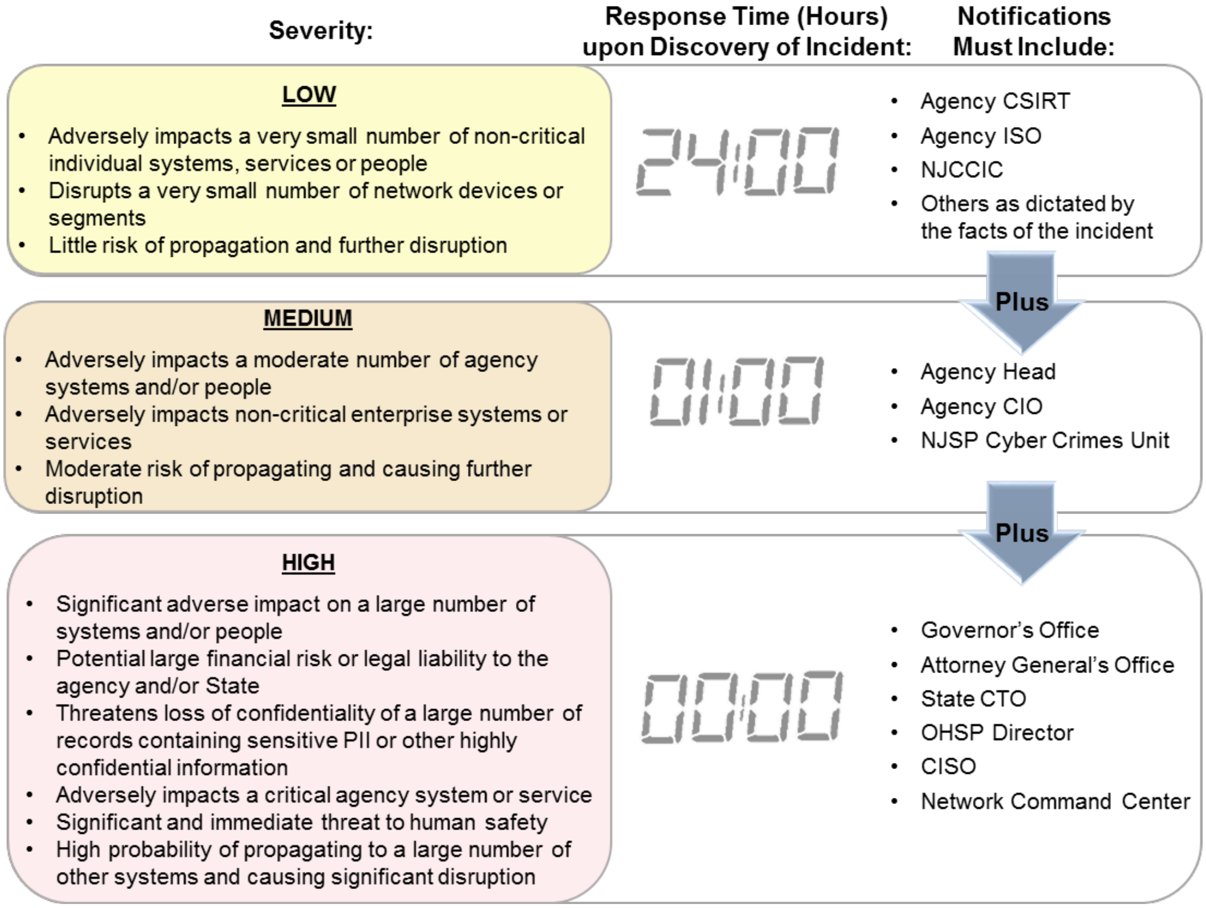
The policy directs agencies to report all incidents to the NJCCIC and describes the process for reporting, managing, and escalating to the appropriate stakeholders.[51] All reports of incidents are collected by NJCCIC and entered into a centralized reporting system for analysis "to identify trends or outbreaks that may require changes to security controls and/or policies to reduce the risk of future occurrences."[52]

The agency CSIRT is responsible for classifying incidents according to the below categories. This approach to classifying cyber incidents provides a standardized means to track incidents across the enterprise, as well as measure frequency and types of incidents.[53]

Table 1. New Jersey Cyber Incident Classification Categories

Category	Name	Description
Cat 0	Security Testing	This category is used during agency-approved vulnerability testing.
Cat 1	Unauthorized Access	Individual gains logical or physical access without authorization to an agency network, system, application, private or restricted data, or other information asset.
Cat 2	Denial of Service (DoS)	An attack that prevents or impairs the normal authorized functionality of agency networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Cat 3	Malicious Code	Installation of malicious software (e.g., virus, worm, Trojan horse, ransomware, or other code-based malicious entity) that infects an agency operating system or application.
Cat 4	Improper Usage	A user violates the Acceptable Use Policy or other agency or state policies.[54]
Cat 5	Scans, Probes, Attempted Access	Any activity that seeks to access or identify an agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or DoS.
Cat 6	Investigation	Unconfirmed incidents that are potentially malicious, or anomalous activity, deemed by the reporting entity to warrant further review.
Cat 7	Data Breach	A data breach is: • The compromise of the confidentiality of personally identifiable information (PII) • Loss of data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of PII • Access to PII for an unauthorized purpose • Access to PII that is in excess of authorization

In addition to the classification of incidents listed above, incidents are also described in terms of levels of severity (low, medium, or high), with associated reporting requirements (see Figure 5 below). "The severity of an information security incident determines the priority and resources necessary to handle the incident" as well as "the timing and extent of the response, the documentation and communications."[55] Assigning a level of severity to an incident is a subjective process, but agencies consider such factors as threat to human safety, scope of the impact (e.g., number of critical systems, services), sensitivity of the information (e.g., PII), and legal obligations and risks, among others.[56]



Severity:	Response Time (Hours) upon Discovery of Incident:	Notifications Must Include:
LOW • Adversely impacts a very small number of non-critical individual systems, services or people • Disrupts a very small number of network devices or segments • Little risk of propagation and further disruption	24:00	• Agency CSIRT • Agency ISO • NJCCIC • Others as dictated by the facts of the incident
MEDIUM • Adversely impacts a moderate number of agency systems and/or people • Adversely impacts non-critical enterprise systems or services • Moderate risk of propagating and causing further disruption	01:00	Plus • Agency Head • Agency CIO • NJSP Cyber Crimes Unit
HIGH • Significant adverse impact on a large number of systems and/or people • Potential large financial risk or legal liability to the agency and/or State • Threatens loss of confidentiality of a large number of records containing sensitive PII or other highly confidential information • Adversely impacts a critical agency system or service • Significant and immediate threat to human safety • High probability of propagating to a large number of other systems and causing significant disruption	00:00	Plus • Governor's Office • Attorney General's Office • State CTO • OHSP Director • CISO • Network Command Center

Figure 5. Levels of Severity and Notification Requirements

Once an incident is reported to the CSIRT, members act to:

- Validate the reported incident,
- Determine the type, severity, and priority of the incident, and
- Notify the CSIRT coordinator or an authorized designee of the incident.

The agency CIO, ISO, or an authorized designee will act as the Incident Coordinator, determine which CSIRT members play an active role in the investigation and:

- Coordinates the agency's response efforts,
- Engages auxiliary agencies and resources as necessary,
- Escalates incidents to executive management as appropriate,
- Monitors progress of the response,
- Ensures evidence gathering, chain of custody, and preservation is appropriate, and
- Prepares a written summary of the incident and corrective action taken.[57]

If an incident is too large for the agency CSIRT to address, the NJCCIC provides incident response assistance. However, if the CSIRT determines the agency has experienced a data breach, the agency is required to notify the NJCCIC in accordance with the New Jersey Identity Theft Prevention Act.[58] The agency leader, ISO, and CIO should also be notified. The NJCCIC, in turn, notifies the State Police Cyber Crimes Unit and the Office of the Attorney General "for legal counsel and guidance in determining the agency's notification responsibilities and response process."[59]

V. Information Sharing

Strategy & Planning
Workforce & Education
Budget & Acquisition
Information Sharing
Risk Identification & Mitigation
Incident Response

The Challenge:

How to engage across multiple organizations to share cybersecurity-related information?

Features of New Jersey's Governance Approach:

- An array of governance mechanisms enables different types of information sharing across government, public, and private organizations.
- NJCCIC is the central information sharing body in the state.
- Two formal bodies, created by law, include private sector stakeholders to raise cybersecurity issues to the attention of executive branch leaders.

New Jersey utilizes an array of governance mechanisms to share different types of information across government, public, and private organizations (see Table 2 below for a summary of various information sharing entities).

Table 2. Summary of Information Sharing Entities

Information Sharing Entities	Type of Information Shared	Target Audience
NJCCIC	Cybersecurity operational and intelligence information	State, local, and federal governments; private sector entities
FS-ISAC	Cyber threats and intelligence information related to financial services industry	Private sector financial institutions and state government (police, attorney general)
DSPTF	Cyber risks to essential state/local services (such as healthcare, transportation, telecommunication services)	State government and the public
IAC	Cybersecurity trends and best practices related to critical infrastructure	Private sector critical infrastructure owner/operators

The NJCCIC is the central cybersecurity information sharing and analysis organization in the state, as well as the hub for cyber operations and resources. The NJCCIC is located at the Regional Operations Intelligence Center (ROIC), which is operated by the Division of State Police and serves as the state's fusion center and emergency operations center.[60] The NJCCIC monitors the state's network for possible cyber-attacks and identifies and analyzes data to determine type of threat, level of severity of threat, threat sources, and potential impacts to stakeholders. The NJCCIC then shares that data and analysis with various stakeholders. In addition to the NJCCIC, New Jersey utilizes a task force and committee to incorporate private sector perspectives on information sharing.

The state's CISO leads the NJCCIC, which is comprised of "appropriate representatives of State entities, including the [OHSP], Office of the Attorney General, Division of State Police, and [OIT] as well as local, county and federal partners and private sector entities as deemed appropriate by the Director of [OHSP]."[61] The NJCCIC includes stakeholders from the public and private sectors, including more than 39 states, 42 federal agencies, state executive departments and agencies, local governments, 13 countries (such as the United Kingdom, Australia, and Germany), and many companies.[62]

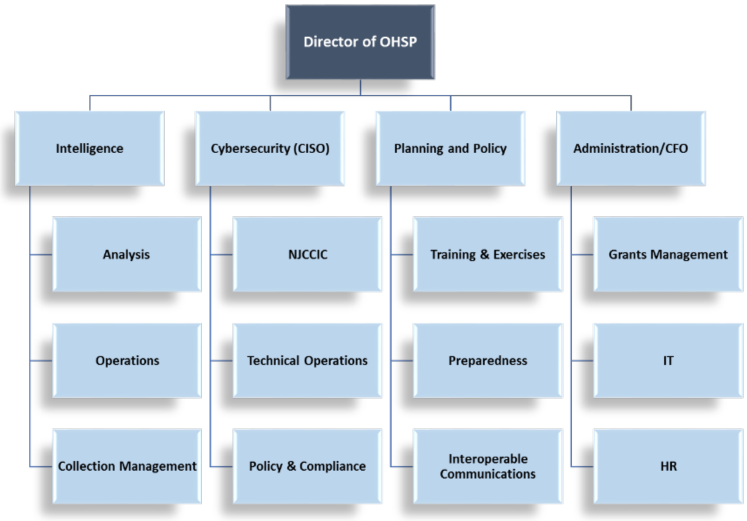


Figure 6. New Jersey Office of Homeland Security and Preparedness[63]

The NJCCIC was intentionally designed as an information sharing body to quickly pass information along to a variety of public and private stakeholders (see Figure 7 below). Within the NJCCIC, the Security Engineering and Cyber Operations (SECOPS) monitors the state's network for attacks. The SECOPS assesses the attacks, vetting them to determine if they are important enough to pass along to NJCCIC stakeholders. The partnerships bureau pushes information out to NJCCIC stakeholders.

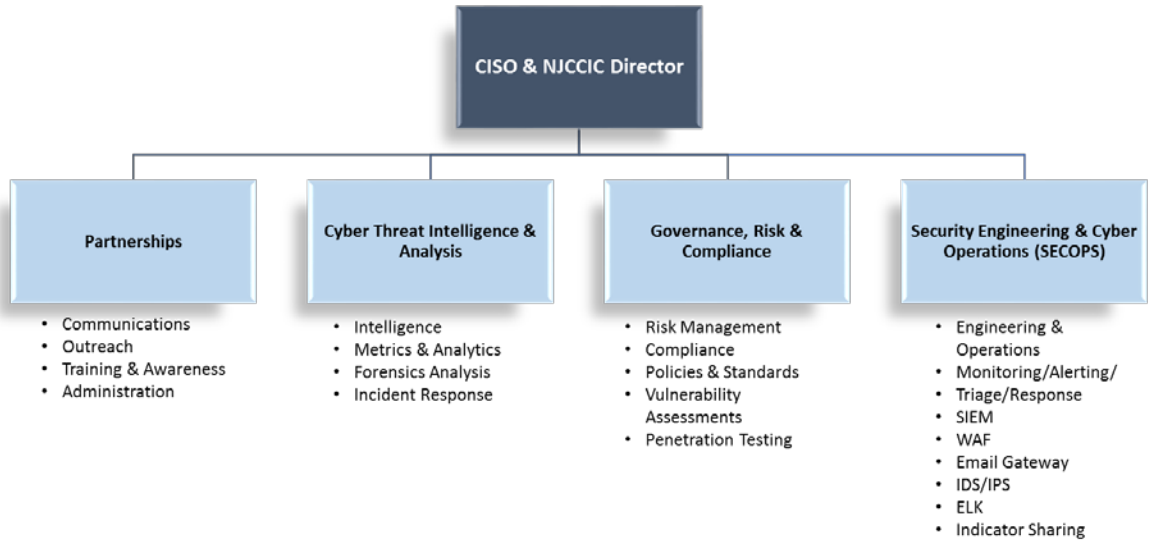


Figure 7. NJCCIC Organizational Chart (as of September 2017)

One way the NJCCIC engages with private sector partners is though the FS-ISAC. Reflective of the large financial services industry in New Jersey, which grew in size and scale following the 9/11 attacks in New York City, the NJCCIC formed a partnership with the FS-ISAC "to share and analyze cyber threat information on behalf of New Jersey's banking institutions."[64] The terms of the NJCCIC/FS-ISAC agreement call for NJCCIC cyber threat analysts to "correlate data from various global financial institutions to identify trends, adversary tactics and vulnerabilities." [65]

In addition, there are two formal bodies with information sharing responsibilities—a task force and a committee—created by law that include private sector participants. The task force and committee provide an opportunity for private/public discussion and information sharing between state officials and private sector stakeholders. In 2001, the legislature passed the New Jersey Domestic Security Preparedness Act, which established the DSPTF. and the IAC. The law is significant because it offers two formal mechanisms for private sector stakeholders to raise cybersecurity issues to the attention of executive branch leaders.

The DSPTF was originally created to coordinate and supervise all activities related to domestic preparedness for a terrorist attack. In 2015, the former OHSP Director Chris Rodriguez expanded the DSPTF's mission to include cybersecurity.[66] The DSPTF resides within the OHSP, meets monthly, and liaisons with the federal Homeland Security Council.[67] The DSPTF is comprised of nine members: the Superintendent of State Police or designee, the Attorney General or designee, the Adjutant General of Military and Veterans' Affairs or designee, the Commissioner of Transportation or designee, the Commissioner of Health and Senior Services or designee, the Coordinator of the Office of Recovery and Victim Assistance, and three public members appointed by the Governor, with the advice and consent of the Senate.

DSPTF duties include identifying and assessing "potential risks to the domestic security and well-being of New Jersey's citizens, including risks to, and disruptions of, essential State and local infrastructures, transportation networks, public and private telecommunications and information networks, financial systems and networks, the delivery and availability of essential health care services, and the potential impact of terroristic chemical, biological and nuclear attacks or sabotage."[68]

In addition to the DSPTF, the law established the IAC to act as a liaison to private industry and state and local officials "regarding domestic preparedness and the respective roles and responsibilities of the public and private sectors…"[69] IAC members include representatives from "gas, water, electric and utilities, nuclear facilities, and the telecommunications, transportation, health care, chemical, and pharmaceutical industries…among others."[70]

The Director of OHSP is co-chair of the IAC, along with a representative from the private sector. The IAC meets once a quarter and includes approximately 40 private sector stakeholders (e.g., Jersey Central Power and Light, Johnson & Johnson, Prudential).[71] The IAC discusses cybersecurity trends and, working with private sector members, authors best practices and guidelines. The IAC is of value to private sector members, in part, because the state of New Jersey can offer security clearances to qualifying businesses, enabling them to read classified information on a need-to-know basis.[72]

VI. Workforce & Education

Workforce & Education
Strategy & Planning
Budget & Acquisition
Risk Identification & Mitigation
Incident Response
Information Sharing

The Challenge:

How does New Jersey work across multiple organizations to shape responses to cybersecurity workforce shortages and education needs?

Features of New Jersey's Governance Approach:

- New Jersey has begun to address some cybersecurity workforce and education issues and the forthcoming Cybersecurity Strategic Plan prioritizes those issues.
- In 2017, New Jersey partnered with the SANS Institute, a nonprofit organization offering online access to free courses.
- OIT policy directs department or agency CISOs to implement and promote information security awareness within their respective organizations.

New Jersey has begun to address some cybersecurity workforce and education issues through discrete initiatives. The forthcoming NJ State Cybersecurity Strategic Plan intends to address workforce development and cybersecurity education issues in a more comprehensive manner. The plan includes, for example, the development of a capable cybersecurity workforce, a cybersecurity curriculum, and a statewide cybersecurity alliance, among other initiatives.[73]

In August 2017, Governor Christie partnered with the SANS Institute, a nonprofit cooperative research and education organization, to establish SANS Cyber Aces Online, an open, free, comprehensive program of online courses. The partnership was formed to address the skills gap in cybersecurity. The coursework was created by the SANS Institute for:

- High school students
- High school teachers and administrators
- College students
- Military veterans
- Active military
- Job seekers
- Career changers

Although the courses are open to anyone, registration is required to participate in the quizzes. SANS donated the courses to the Cyber Centers (called the SANS Cyber Aces Online), and the program provides an overview of the "core concepts needed to assess, and protect information security systems."[74] Example online courses include network fundamentals, operating systems, and system administration.

To address cybersecurity education among state employees, OIT policy directs department or agency CISOs to implement and promote “information security awareness within their respective agency.” [75] In addition, the Director of NJCCIC is directed under OIT policy to draft and implement “an information security awareness and training program to be used by all State agencies.”[76]

VII. Acronyms

Acronym	Definition
CDO	Chief Data Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CS&C	Office of Cybersecurity and Communications
CTO	Chief Technology Officer
CSIRT	Cybersecurity Incident Response Team
DoS	Denial of Service
DHS	Department of Homeland Security
DSPTF	Domestic Security Preparedness Task Force
FFRDC	Federally Funded Research and Development Center
FS-ISAC	Financial Services Information Sharing and Analysis Center
GRCB	Governance Risk and Compliance Bureau
HSSEDI	Homeland Security Systems Engineering and Development Institute
IAC	Infrastructure Advisory Committee
ISO	Information Security Office
IT	Information Technology
NASCIO	National Association of State Chief Information Officers
NJCCIC	New Jersey Cybersecurity & Communications Integration Cell
OHSP	Office of Homeland Security and Preparedness
OIT	Office of Information Technology
OMB	Office of Management and Budget
ROIC	Regional Operations Intelligence Center
SECOPS	Security Engineering and Cyber Operations
SLTT	State, Local, Tribal & Territorial
SAR	Systems Architecture Review

[1] Statistical Atlas, "Overview of New Jersey." Data based on US Census Bureau 2010 census. Available: https://statisticalatlas.com/state/New-Jersey/Overview#nav-map/metro-area. Retrieved October 2017.

[2] Information regarding elected officials and state cybersecurity executives was validated in November 2017. "Fast Fact" details were collected in October 2017.

[3] New Jersey Legislature, General Information: Our Legislature. Available: http://www.njleg.state.nj.us/legislativepub/our.asp.

[4] Statistical Atlas, "Occupations in New Jersey." Data based on US Census Bureau 2010 census. Available: https://statisticalatlas.com/state/New-Jersey/Occupations. Retrieved October 2017.

[5] New Jersey Council of County Colleges. Available: http://www.njccc.org/.

[6] State of New Jersey, Office of the Secretary of Higher Education. Available: http://www.nj.gov/highereducation/colleges/schools_sector.shtml.

[7] New Jersey Economic Development Organization. Available: http://www.choosenj.com/key-industries.

[8] The OIT was established by Executive Order No. 84 (1984), Executive Order No. 87 (1998), and Executive Order No. 42 (2006). All functions, powers, and duties from the Executive Orders were codified in OIT through the Office of Information Technology Reorganization Act of 2007, N.J.S.A. 52:18A-224 et seq.

[9] C.52:18A-225(7)(g), ftp://www.njleg.state.nj.us/20062007/PL07/56_.HTM.

[10] New Jersey Department of Law and Public Safety, "Analysis of the New Jersey Budget: Fiscal Year 2017-2018." Available: http://www.njleg.state.nj.us/legislativepub/budget_2018/LPS_analysis_2018.pdf.

[11] Interview with Mike Geraghty, New Jersey CISO and Director of NJCCIC, September 1, 2017.

[12] Ibid.

[13] State of New Jersey, "Enterprise Information Security Policies and Standards," January 2017.

[14] Ibid. The CISO and Director of the NJCCIC is also responsible for developing, implementing, and measuring the performance of the information security program by "setting strategic information security planning across the Executive branch…, publishing and maintaining statewide information security policies and standards and providing cybersecurity subject matter expertise to state agencies.…"

[15] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.

[16] Department of Homeland Security Advisory Council, "Final Report of the Cybersecurity Subcommittee, Part II – State, Local, Tribal & Territorial (SLTT)." (2016, June). Available: https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_SLTT_FINAL_Report.pdf.

[17] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.

[18] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.

[19] Ibid.

[20] State of New Jersey, Office of Homeland Security and Preparedness, Organization overview, https://www.njhomelandsecurity.gov/organization.

[21] National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure, Draft Version 1; NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; International Standards Organization 27002:2013 Information Technology — Security Techniques — Code of Practice for Information Security Controls; Center for Internet Security Top 20 Critical Security Controls; Cloud Security Alliance Cloud Controls Matrix; applicable laws and regulatory requirements, lessons learned, industry best practices, and other New Jersey state government business and technology-related considerations.

[22] Information security policies and standards are authorized under N.J.S.A. 52:18a-227, which defines the role of the New Jersey Office of Information and Technology (NJOIT) in the development of policies and standards governing the use of technology by state agencies.

[23] State of New Jersey, "Enterprise Information Security Policies and Standards," January 2017.

[24] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017. Available: http://www.nj.gov/highereducation/colleges/schools_sector.shtml.

[25] Interview with David Weinstein, New Jersey CTO, September 6, 2017.

[26] Ibid.

[27] Interview with Mike Geraghty, New Jersey CISO and Director of the NJCCIC, September 1, 2017.

[28] New Jersey Department of Treasury, Joint Circular No. 18-03-OMB/DPP/OIT, "Procurements of Information Technology (IT) Hardware, Software, Subscription-based Solutions and Related Services and Non-IT Equipment," August 22, 2017. Available: http://www.state.nj.us/infobank/circular/cir1803.pdf.

[29] Ibid.

[30] Interview with David Weinstein, New Jersey CTO, September 6, 2017.

[31] New Jersey Department of Treasury, Joint Circular No. 18-03-OMB/DPP/OIT, "Procurements of Information Technology (IT) Hardware, Software, Subscription-based Solutions and Related Services and Non-IT Equipment," August 22, 2017. Available:

http://www.state.nj.us/infobank/circular/cir1803.pdf.

[32] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.

[33] Interview with Mike Geraghty, New Jersey CISO and Director of the NJCCIC, September 1, 2017.

[34] Ibid.

[35] NJ OIT Technology Circular (Policy No. 16-05-NJOIT). "System Architecture Review Policy." December 12, 2016. Available: http://www.nj.gov/it/docs/ps/16-05-NJOIT_System_Architecture_Review_Policy.pdf.

[36] Ibid.

[37] The image is adapted from the OIT Technology Circular regarding SAR process, published in December 2016.

[38] New Jersey Office of the Governor, Executive Order 225, "Governor Chris Christie Signs E.O. To Bolster NJ's Cyber Security, IT Enterprise," June 1, 2017. Available: http://www.nj.gov/governor/news/news/552017/approved/20170601a.html.

[39] State of New Jersey Technology Circular, "System Architecture Review Procedure," New Jersey Office of Information Technology, Policy No. 16-05-P1-NJOIT, December 12, 2016. Available: http://www.nj.gov/it/docs/ps/16-05-NJOIT%20P%20System%20Architecture%20Review%20Procedure.pdf.

[40] Ibid.

[41] Ibid.

[42] State of New Jersey, "Enterprise Information Security Policies and Standards," January 2017.

[43] Ibid.

[44] State of New Jersey, "Cybersecurity Incident Response Plan," v1.0, February 2017.

[45] Ibid. The CISO must update the plan at least once a year.

[46] Ibid.

[47] Ibid. Furthermore, "incidents may result from intentional or unintentional actions and may include loss or theft of agency information assets, unauthorized access to agency information assets, introduction of malicious code, or the failure of system security functions to perform as expected."

[48] Ibid.

[49] Ibid.

[50] State of New Jersey, "Enterprise Information Security Policies and Standards," January 2017.

[51] Ibid.

[52] Ibid.

[53] Ibid.

[54] Ibid. Examples of incidents a team might handle are users who:

- Download and install unapproved software, hacking tools, etc.
- Access or download materials in violation of the Acceptable Use policy
- Send spam promoting a personal business
- Email harassing messages to coworkers
- Set up an unauthorized website on one of the agency's computers
- Use file or music sharing services to acquire or distribute pirated materials
- Transfer sensitive materials from the agency to external locations

[55] State of New Jersey, "Enterprise Information Security Policies and Standards," February 2017.

[56] Ibid. Agencies shall consider the following factors when determining the severity of an incident:

- Threat to human safety
- Scope of impact—number and criticality of systems, services, agencies, and people affected
- Financial impact to the agency or state—loss of revenue, financial penalties, etc.
- Sensitivity of the information—personally identifiable information or other confidential data
- Probability of propagation—likelihood that the malware or negative impact will spread or propagate to other systems or agencies
- Reputational impact to the state or an individual agency
- Legal obligations and risks—notification requirements, regulatory issues, potential lawsuits, etc.

[57] State of New Jersey, "Cybersecurity Incident Response Plan," v1.0, February 2017.

[58] Ibid. Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

[59] Ibid.

[60] The functions of the ROIC are threefold: conducting watch floor operations (Watch Ops), real-time tactical intelligence analysis (Analysis), and tracking assets (Asset Management and Coordination). During daily operations, these functions are performed to create a complete picture of the current operating environment throughout the state of New Jersey, including external factors that may also present immediate concerns (terrorism, severe weather events, gang or drug problems in neighboring states, etc.), as well as the resources available to address them. During crisis operations, these same functions remain paramount, albeit with much greater immediacy of information flow and expanded outreach to and integration with external agencies and federal partners. Drawing upon its resources and partners, the ROIC remains the center of gravity for the creation of a comprehensive common operating picture of relevant

events and happenings within the state.

[61] New Jersey Office of the Governor, Executive Order 178, “Governor Christie Takes Action to Defend New Jersey and its Infrastructure from Cybersecurity Threats,” May 20, 2015. Accessible: https://www.cyber.nj.gov/njccic-executive-order-signing/.

[62] Interview with Chris Rodriguez, former Director of New Jersey Office of Homeland Security and Preparedness (OHSP), September 15, 2017.

[63] State of New Jersey, Office of Homeland Security and Preparedness, Organization, https://www.njhomelandsecurity.gov/organization.

[64] Nussbaum, Brian. “State-Level Cyber Security Efforts: The Garden State Model.” *Center for Internet and Society at Stanford Law School*. August 24, 2015. Available: http://cyberlaw.stanford.edu/blog/2015/08/state-level-cyber-security-efforts-garden-state-model.

[65] Ibid.

[66] Interview with Chris Rodriguez, former Director of New Jersey Office of Homeland Security and Preparedness (OHSP), September 15, 2017.

[67] Ibid.

[68] New Jersey C.App.A:9-67. Available: http://www.njleg.state.nj.us/2000/Bills/pl01/246_.pdf.

[69] Ibid.

[70] Ibid.

[71] Interview with Chris Rodriguez, former Director of New Jersey Office of Homeland Security and Preparedness (OHSP), September 15, 2017.

[72] Ibid.

[73] Taken from conversation with Mike Geraghty, New Jersey CISO and Director of the NJCCIC, September 1, 2017.

[74] SANS CyberAces.org, “Your gateway to cybersecurity skills and careers,” Accessed August 21, 2017, http://cyberaces.org/.

[75] State of New Jersey Technology Circular, “Enterprise Information Security Management,” New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.

[76] Ibid.