New Jersey Civilian Cyber Resilience Corps Charter

Introduction

The State of New Jersey recognizes the escalating and increasingly sophisticated cybersecurity threats that pose a significant risk to its public and private sectors. These threats target critical infrastructure, government services, businesses of all sizes, and individual citizens, potentially leading to substantial economic losses, disruption of essential services, and adverse impacts on public health and safety.

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) is a division within the New Jersey Office of Homeland Security and Preparedness and is charged with leading and coordinating the State's cybersecurity efforts, building resilience against cyber threats, and acting as the central civilian interface for cybersecurity information sharing, threat intelligence, and incident reporting and response. A volunteer New Jersey Civilian Cyber Resilience Corps has been established to augment the efforts of the NJCCIC and further strengthen New Jersey's cyber resilience. The New Jersey Civilian Cyber Resilience Corps (hereinafter referred to as the "Cyber Corps"), operating under the auspices of the NJCCIC, will leverage the skills and expertise of volunteer cybersecurity and technology professionals from across the State to provide critical support in areas such as incident response and recovery, vulnerability assessments and threat modeling, target hardening, information sharing, and cybersecurity training. By formally organizing and coordinating these volunteers, New Jersey creates a readily available resource that augments the State's ability to assist public and private sector entities in enhancing their cybersecurity posture and effectively responding to and recovering from cyber incidents.

This charter establishes a general framework for the creation, structure, and operation of the Cyber Corps. It is intended to provide foundational guidance while allowing flexibility to adapt to evolving cybersecurity needs, operational lessons learned, and changes in policy or law. Certain provisions within this charter may be revised or updated over time.

Mission and Purpose

The Cyber Corps is established as a volunteer-based cybersecurity force intended to augment the State's cyber defense and incident response capabilities. Its primary purpose is to assist public and private entities (hereinafter referred to as "service recipients") in improving their cyber resilience and recovering from adverse cyber events. The Cyber Corps volunteers (hereinafter referred to as "Corps Members") serve in a non-paid, civilian capacity to provide expert cybersecurity and technical support during significant incidents and to bolster ongoing preparedness efforts. By leveraging skilled volunteers, the Cyber Corps enhances New Jersey's ability to prevent and mitigate cyberattacks.

Authorities and Organizational Structure

The Cyber Corps is established under the auspices of the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), operating within the New Jersey Office of Homeland

Security and Preparedness (NJOHSP). This initiative is authorized by the New Jersey Domestic Security Preparedness Task Force (DSPTF) pursuant to its mandate to coordinate and strengthen the State's preparedness for security threats. The NJOHSP Director, who chairs the DSPTF, authorizes the NJCCIC Director to create and oversee the Cyber Corps as an official NJOHSP-sponsored volunteer program. The Cyber Corps functions as an operational component of the NJCCIC, ensuring it is integrated into the State's existing cybersecurity infrastructure and reporting chain. See Appendix A for more details on the authorities enabling the creation of the Cyber Corps.

Governance and Oversight

Oversight Structure: Governance of the Cyber Corps is vested in the NJCCIC, NJOHSP, and the DSPTF. The NJCCIC Director is responsible for setting the strategic direction of the Cyber Corps, integrating it into the NJCCIC's programs, supervising the Cyber Corps' operations, and ensuring compliance with all applicable state and federal statutes, executive orders, and state policies and standards. Strategic oversight is provided by the NJOHSP Director and the DSPTF, which will receive regular updates on the Cyber Corps' development and activities and may issue broad directives or authorize deployments in extraordinary circumstances. This dual oversight structure ensures both vertical integration within NJOHSP/NJCCIC and horizontal coordination across relevant State agencies. High-level coordination between NJOHSP/NJCCIC and other State entities, such as the New Jersey Office of Emergency Management (NJOEM), the New Jersey Office of Information Technology (NJOIT), the New Jersey State Police (NJSP), and the New Jersey National Guard (NJNG), will be facilitated through the DSPTF, thereby embedding the Cyber Corps into the State's overall security preparedness strategy and the Cyber Incident Annex to the State Emergency Operations Plan.

Advisory Council: A Cyber Corps Advisory Council will be established to provide expert guidance, foster public-private collaboration, and ensure the program's activities remain aligned with best practices. The Advisory Council will be led by the NJCCIC Director and include cybersecurity leaders from both the public and private sectors. At a minimum, the council will include: the NJCCIC Director, one member representing another public sector stakeholder (e.g., NJOIT, NJOEM, or local government), and at least two members from the private sector, such as cybersecurity industry experts or critical infrastructure IT leaders. Additional members from academia or non-profit cyber initiatives may be included, as deemed appropriate by the NJCCIC Director, to leverage broad expertise. The Advisory Council's role is advisory and non-binding, as it will review the Cyber Corps policies, training plans, and operational procedures and make recommendations for improvements. This body will meet periodically to evaluate the Cyber Corps' progress, suggest updates to volunteer eligibility requirements, assist in developing training curricula, and facilitate partnerships. By consulting this expert council, the NJCCIC Director can develop well-informed rules and guidance for the Cyber Corps in line with the evolving cyber threat landscape.

Funding and Budget: The Cyber Corps will initially be funded from the NJCCIC's current state cyber budget allocation and applicable state and federal grant funds. As necessary, additional

sources of funding will be explored to sustain and support the Cyber Corps in carrying out its mission.

Recruitment, Application Process, and Volunteer Eligibility Requirements

Recruitment: The NJCCIC is responsible for recruiting qualified volunteers to serve in the Cyber Corps. Recruitment efforts are to include outreach via NJCCIC's membership network, information sessions at cybersecurity and technology conferences, outreach to technology companies and universities, and coordination with professional associations (e.g., ISC², ISACA, NJGMIS, etc.).

Application Process: The NJCCIC will develop a standardized application and screening process. Applicants will submit credentials and may be required to take a skills assessment exam to demonstrate technical competency, which could involve practical evaluations or quizzes on cybersecurity and IT fundamentals aligned with the program's needs. The Advisory Council may assist in developing these assessments and setting the standards for eligibility requirements. Once an applicant meets all requirements and passes screening, at the discretion of the NJCCIC and as needs dictate, they may be onboarded as a Cyber Corps Volunteer.

Volunteer Eligibility Requirements: Applicants to the Cyber Corps must possess a baseline of cybersecurity and technology experience and expertise, trustworthiness, and the following requirements:

- **Professional Experience:** A minimum threshold of practical cybersecurity and technology experience (e.g., 3 years in roles conducting computer and network defense operations, systems administration and engineering, network administration and engineering, incident response, risk and vulnerability assessments, threat analysis and intelligence, etc.)

- **Technical Competency:** Demonstrable knowledge and experience of operating systems, networking, systems administration, cybersecurity defense tools and technologies, incident handling, etc. Possession of industry-recognized certifications (e.g., A+, Network+, Security+, SecurityX, CASP+, CCIE, CISSP, OSCP, Cloud+, etc.) or equivalent training is strongly preferred.

- **Consent to Screening:** The applicant will be required to consent to and pass a criminal background check conducted by NJOHSP.

- **Employer Support:** If a volunteer is employed, they should provide a letter of employer support for their participation. Employer support is encouraged to ensure that volunteers can be made available for training or emergency response without undue conflict with their primary jobs.

Volunteer Agreement: Every accepted volunteer will enter into a formal Cyber Corps Member Service Agreement with the NJCCIC/NJOHSP on behalf of the State. This agreement defines the relationship and expectations. At a minimum, the agreement will include:

- **Scope of Service and At-Will Nature:** The Cyber Corps Member Service Agreement will clarify that the individual is serving as a volunteer, not as a paid employee or contractor of the State, and either party may terminate the volunteer status at any time. The volunteer has no employment rights or benefits and is not an agent of the State for legal or financial obligations.

- **Confidentiality Agreement:** A Non-Disclosure Agreement (NDA) requires the Cyber Corps Member to protect any sensitive or confidential information encountered during service in the Cyber Corps, such as personally identifiable information, State information, service recipient data, third-party data, or incident details they may access.

- **Conflict of Interest Disclosure:** Cyber Corps Members must disclose any potential conflicts of interest (e.g., if their employer is a vendor to a potential service recipient, or if they have other affiliations that might affect impartiality). The agreement will stipulate that Cyber Corps Members avoid situations where private interests could interfere with their Cyber Corps duties.

- **Liability and Indemnification Acknowledgment:** The agreement will outline liability protections and include the Cyber Corps Member's acknowledgment that they are protected under applicable state and federal laws that provide protections for volunteers and must exercise due care. Further, Cyber Corps members are covered under the State of New Jersey's Health and Accident Insurance for Volunteers Policy.

- **Adherence to Rules:** The Cyber Corps Member agrees to comply with all applicable policies, rules, and guidelines that the NJCCIC issues for the Cyber Corps, including operational protocols, safety procedures, use of state equipment policies, etc.

The Cyber Corps Member Services Agreement must be signed by the Cyber Corps Member and the NJCCIC Director or an authorized designee to document mutual understanding of the roles and protect the interests of both the volunteer and the state.

Volunteer Training and Development

Orientation: Upon acceptance into the Cyber Corps, new members will undergo an orientation program led by NJCCIC staff. This introduction will cover the Cyber Corps mission, chain of command, communication procedures, use of any provided equipment, tools, technologies, or accounts, and reinforcement of confidentiality and ethics requirements. New members will also be issued a credential letter identifying them as Cyber Corps Members for use when on official assignments.

Training and Exercise: After onboarding, the NJCCIC will provide appropriate initial training to prepare Cyber Corps Members for deployment. The standardized training modules comprise the cybersecurity standards and policies included in the State Information Security Manual (SISM), State incident response protocols, the Cyber Incident Annex to the State Emergency Operations Plan, relevant New Jersey laws and regulations, secure handling of evidence, and tools that the

Cyber Corps uses. Volunteers may be required to complete specific online courses or in-person workshops offered by the NJCCIC.

To maintain operational readiness, all Cyber Corps Members are required to complete annual training programs organized by the NJCCIC and to participate in Cyber Corps exercises and workshops. At a minimum, all Cyber Corps Members are required to attend at least two NJCCIC-provided training programs and exercises annually. These events could include in-person or remote classes, formal exercises, tabletop simulations, or technical workshops. Training topics will be selected to keep Cyber Corps Members updated on emerging threats, new defensive techniques, improvements in incident response, and other relevant topics. In addition, hands-on live fire training exercises and simulations utilizing the NJCCIC cyber range will be conducted to ensure Cyber Corps Members have the necessary knowledge and skills to carry out their duties.

Certifications: The NJCCIC will encourage and sponsor Cyber Corps Members to pursue certifications relevant to their duties at the Cyber Corps.

Roles and Responsibilities

The Cyber Corps shall be authorized to provide the following services to eligible beneficiaries:

- Cybersecurity assessments;
- Target hardening and resilience improvement;
- Incident response and recovery support;
- Cybersecurity awareness and training;
- Cybersecurity strategy and policy development; and
- Information sharing and threat intelligence.

Cyber Corps Members shall act under the direction of the NJCCIC and adhere to all protocols and guidelines established for the safe and effective delivery of services.

Operations and Deployment

Cyber Corps Members may be deployed in accordance with NJCCIC protocols. Deployment may occur in response to:

- Requests for assistance from public sector entities, critical infrastructure providers, or other stakeholders;
- State-declared cybersecurity emergencies; or
- Identified threats or vulnerabilities requiring immediate action.

All operations shall be carried out under the supervision of the NJCCIC, and all activities must comply with applicable laws, regulations, and agreements.

Requests for Cyber Corps Services: Authorized officials of an eligible entity can request Cyber Corps assistance by contacting the NJCCIC through established NJCCIC channels, including phone

(1-833-465-2242), email (njccic@cyber.nj.gov), or website (cyber.nj.gov). Emergency requests can be made 24/7 by calling 1-866-472-3365. Requestors must provide information about the nature of the cybersecurity issue and affirm that their request meets the criteria for volunteer deployment.

Deployment Criteria: The NJCCIC considers factors such as the severity, scope, and impact of the cyber incident, the resource needs of the affected entity, the availability of Cyber Corps resources, and the request's alignment with the Cyber Corps' mission when deploying and prioritizing Cyber Corps services. Proactive deployments for cyber resilience services may also be provided for cybersecurity assessments, risk reduction, security posture improvements, and cybersecurity training and awareness delivery.

Cyber Corps Member Acceptance of Assignments: Participation in any deployment is voluntary. Cyber Corps Members will be asked in writing to accept a deployment assignment, and no Cyber Corps Member will be compelled to serve on a specific mission. Cyber Corps Members are free to decline an activation request for any reason (e.g., work conflicts, personal obligations, etc.).

Scope of Deployment Activities: When deployed, Cyber Corps Members will operate under the coordination of the NJCCIC and in partnership with the requesting entity's IT staff, incident response team, or other authorized officials or designees. Cyber Corps Members may perform computer and network defense operations, including actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and computer networks. Computer and network defense operations include incident response activities, such as detection and analysis, containment, eradication, and recovery from a cybersecurity incident. Cyber Corps Members may also serve in advisory roles if full hands-on involvement is not needed. Each deployment will have a designated NJCCIC point of contact to whom volunteers report and coordinate.

Duration and Demobilization: Deployments are generally short-term engagements, lasting until the immediate crisis is stabilized or the requested support has been completed. The NJCCIC will monitor ongoing incidents and may rotate Cyber Corps Members if an incident is protracted. A formal demobilization will occur at the conclusion of each deployment, including a debrief with the mobilized Cyber Corps Members to capture lessons learned and a report generated for record-keeping and after-action review.

Service Recipient Eligibility and Agreements

Eligible Cyber Corps Service Recipients: Entities eligible to receive assistance from the Cyber Corps are broadly referred to as Service Recipients. They consist of state and local government entities, including all governmental entities below the federal level, such as state departments, agencies, authorities, commissions, state and county colleges, counties, municipalities, school districts, public charter schools, and county and municipal utility authorities; and privately owned organizations operating critical infrastructure or key resources in the State (such as healthcare systems, utilities, transportation networks, etc.). The NJCCIC, under guidance from DSPTF and the Advisory Council, may further refine eligibility criteria focusing on under-resourced or high-

risk organizations that lack adequate cybersecurity capabilities. Small and medium-sized businesses that are not designated as critical infrastructure are generally not direct beneficiaries, unless there is a nexus to state security, or they are part of a larger supply chain incident.

Service Recipient Agreement: Before Cyber Corps Members are deployed to an incident or project, the Service Recipient will enter into an agreement with NJCCIC/NJOHSP to outline the terms of assistance. This Service Recipient Agreement protects both the volunteers and the beneficiary. Key elements include:

- Confidentiality of Information;
- Volunteer Access and Safety;
- Waivers of Liability and Indemnification;
- Data Breach Notifications;
- Intellectual Property and Results; and
- No Cost (or Cost Recovery Terms).

In urgent cases, email correspondence or an executive verbal agreement will suffice initially, but a written agreement will follow as soon as feasible.

Confidentiality and Information Security

Cyber Corps Members, the NJCCIC, and the Service Recipient are required to protect each other's confidential information in accordance with all applicable state and federal laws, regulatory requirements, policies, and contractual terms. Confidential information includes, but is not limited to, all information related to computer and network defense operations, such as incident response and recovery activities conducted as a part of a Cyber Corps engagement.

The obligation to maintain the confidentiality of the Cyber Corps' and the beneficiary's confidential information is conditioned upon and subject to the State's obligations under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 et seq. (OPRA), The New Jersey Domestic Security Preparedness Act - P.L.2003, c.246, the laws requiring incident reporting to the NJCCIC, P.L.2023, c.19 (C.52-17B-193.2), the New Jersey common law right to know, and all other applicable state and federal statutes.

> **New Jersey Open Public Records Act (N.J.S.A. 47:1A-1 et seq.)**: Cyber Corps engagements would inherently include administrative or technical information, which, if disclosed, would jeopardize the computer security of the beneficiary and the NJCCIC. As such, to the extent permitted by law, all information, records, notes, written comments, reports, or analyses generated in or in the execution of a Cyber Corps engagement shall be treated and deemed as exempt from public disclosure under OPRA.
>
> **Domestic Security Preparedness Task Force Records:** In accordance with the New Jersey Domestic Security Preparedness Act, N.J.S.A. APP. A: 9-74 and approval by DSPTF, any record held, maintained, or kept on file by the NJCCIC related to the Cyber Corps

engagements shall be treated and deemed as “records of the Task Force exempt from public disclosure under OPRA.”

Incidents Reported to the NJCCIC: Pursuant to P.L.2023, c.19 (C.52:17B-193.2 et seq.), any cybersecurity incident notification submitted to the NJCCIC is deemed confidential, non-public, and not subject to the provisions of P.L.1963, c.73 (C.47:1A-1 et seq.), commonly known as the Open Public Records Act, as amended and supplemented, and may not be discoverable in any civil or criminal action, and may not be subject to subpoena, unless the subpoena is issued by the New Jersey State Legislature and is deemed necessary for the purposes of legislative oversight.

Information Security: The Cyber Corps will adhere to all policies and standards in the Statewide Information Security Manual necessary to protect the confidentiality, integrity, availability, and privacy of NJCCIC and Service Recipient information and information systems.

Confidential Information Handling: All information encountered or generated by the Cyber Corps in the course of its activities is subject to security controls. This information includes details of cyber incidents, vulnerability assessments, network or personal data from Service Recipients, and Cyber Corps Members' own personal information. Such information will be handled on a need-to-know basis and stored securely within NJCCIC systems. Cyber Corps Members will be instructed and trained on handling protocols (e.g., encrypted communication channels, secure data storage, strong authentication, etc.).

Secure Communication: To protect sensitive information, all Cyber Corps operational communications will use secure channels. The NJCCIC will provide Cyber Corps Members with official email accounts and access to a secure portal for any sensitive communication. All sensitive data will be encrypted in transit and at rest, and robust access controls will be implemented, including multi-factor authentication to restrict access to authorized personnel only. Volunteers will also be expected to practice good operational security (e.g., not discussing sensitive matters in public or with those outside the response effort and reporting any suspected information leaks).

Cyber Corps Member Identities and Personal Information: The Cyber Corps Members' privacy will be safeguarded. Recognizing that malicious actors could target Cyber Corps Members or their employers if their participation became public. To the extent permitted by law, the NJCCIC will treat Cyber Corps Members' personal information (names, contact info, employer, etc.) as confidential. State records listing Cyber Corps Members will be kept internal to the NJCCIC, and the personally identifiable information of Cyber Corps Members will be protected. Cyber Corps Members may choose to self-identify and speak about their service publicly, but the NJCCIC will not release Cyber Corps Member rosters openly. This practice not only protects individuals but also aids recruitment and retention by alleviating concerns over exposure.

Records Management: The NJCCIC will maintain detailed records of each Cyber Corps deployment (e.g., actions taken, data collected, results achieved). Access to these records will be limited to those individuals with a need-to-know basis and proper authority. If the Cyber Corps

compiles written reports for a Services Recipient, those documents will typically be co-owned by the NJCCIC and the Service Recipient and will not be published publicly. Additionally, any after-action reports that summarize incidents for lessons learned will anonymize the Services Recipient and scrub technical details that could be exploited.

Information Sharing: While confidentiality is paramount, appropriate information sharing with trusted partners is still important for cybersecurity. The NJCCIC may share sanitized lessons learned, indicators of compromise, or threat actor techniques, tactics, and practices gleaned from an incident with key stakeholders or the broader cybersecurity community, but only after removing identifying details of the Service Recipient. Information sharing procedures will be based on the federal Cybersecurity Information Sharing Act of 2015 and the State of New Jersey Public Agency and Government Contractor Incident reporting law - P.L. 2023, c.19.

Equipment, Facilities, and Operational Readiness

Equipment Provision: The NJCCIC will ensure that the Cyber Corps has access to the necessary tools and equipment to perform its cybersecurity tasks effectively. The NJCCIC will allocate a set of cyber incident response tools and resources for the Cyber Corps' use, which may include hardware (such as laptops pre-loaded with security software, portable storage devices, forensic disk imaging kits, network analysis appliances, etc.) and software licenses (for endpoint security, malware analysis sandboxes, vulnerability scanning, etc.). Cyber Corps Members will be trained on using any provided technology and must return state-owned equipment when leaving the program or when requested.

Facilities: The primary base of operations for the Cyber Corps will be at the NJCCIC Security Operations Center (SOC) at the Regional Operations and Intelligence Center (ROIC) in West Trenton, NJ. The NJCCIC will ensure a dedicated workspace for Cyber Corps personnel when activated. In addition, the NJCCIC may set up operations at a beneficiary's facilities or authorize Cyber Corps work and training to be conducted remotely, provided secure operations are maintained.

Operational Readiness: The NJCCIC will maintain an up-to-date roster of all active Cyber Corps Members, including their skill specialties, geographic location, and availability. An alert or notification system (such as an SMS or phone tree) will be implemented to rapidly contact Cyber Corps personnel for emergency call-ups.

Cyber Corps Member Protections, Indemnifications, and Waivers of Liability

Volunteers serving in the Cyber Corps are afforded liability protections under both federal and State law, including the Volunteer Protection Act of 1997 and applicable provisions of New Jersey law. These protections ensure that individuals who volunteer their time and expertise in good faith, within the scope of their assigned duties, and in accordance with applicable laws and Cyber Corps program guidelines are shielded from personal liability for acts or omissions that may occur in the course of their service. This legal framework is designed to encourage public service by reducing the risk of personal legal exposure for volunteers who contribute to the cybersecurity and resilience of state and local government systems. These protections do not extend to acts of

willful or criminal misconduct, gross negligence, reckless misconduct, operation of a motor vehicle, or actions involving crimes of violence, sexual offenses, or violations of civil rights laws, or actions taken while under the influence of drugs or alcohol.

Waiver of Liability: In addition to the protections afforded to Cyber Corps Members by applicable state and federal laws, each Services Recipient will be required to sign a Waiver of Liability Agreement that makes clear that all services are offered "as-is" with no guarantees of effectiveness or outcomes, and that the Services Recipient assumes full responsibility for their cybersecurity posture. The agreement waives the Services Recipient's right to hold the NJCCIC, the Cyber Corps, their members, or the State of New Jersey liable for any damages, losses, or claims arising from the provision or non-provision of services. It also requires the Services Recipient to indemnify and defend the Cyber Corps and related parties against any legal claims connected to the services rendered.

Volunteer Access and Safety: The Service Recipient consents to provide assigned Cyber Corps personnel the necessary access to facilities, systems, and information to perform their work. For example, this access may be temporary user accounts, VPN access, or escorted physical access within a facility. The Services Recipient will brief assigned Cyber Corps personnel on any on-site safety or security protocols.

Liability and Indemnification: The agreement will spell out that the State and Cyber Corps Members are not liable for any unintended consequences of the assistance, except in cases of gross negligence or willful misconduct. The Services Recipient agrees not to hold Cyber Corps members or the State responsible for harm caused by a good-faith attempt to assist. Furthermore, the Services Recipient may be asked to indemnify the State and Cyber Corps Members against third-party claims arising from the incident. For instance, if a third party's data is affected, the Service Recipient will handle any claims, not the Cyber Corps. This indemnification for claims related to the assistance provided is a standard protective measure.

Data Breach Notifications: The agreement clarifies that the Services Recipient retains any legal duty to make data breach notifications or comply with applicable regulations, including in the event personal data is compromised. Assistance from the Cyber Corps does not transfer those responsibilities. Cyber Corps personnel can advise on notification procedures, but the obligation lies with the Services Recipient.

Intellectual Property and Results: Any tools or generated reports provided to the Services Recipient (e.g., network scan, forensic analysis, etc.) will be for their use. The Services Recipient's intellectual property (such as proprietary system information) remains protected; likewise, any new analysis or reports produced by the Cyber Corps may be shared with the beneficiary and the NJCCIC but not beyond, except in anonymized form for lessons learned. Protections for the Services Recipient's sensitive information and intellectual property will be explicitly stated.

No Cost (or Cost Recovery Terms): Cyber Corps services are provided at no cost to the Services Recipient. The State will cover any necessary costs, such as specialized software or travel

expenses beyond what Cyber Corps covers, or these will be addressed through prior agreement. In rare cases where cost recovery is considered, it will never exceed the State's direct expenses, will be clearly outlined in policy, and must be agreed to by the Services Recipient before any purchase.

APPENDIX A - AUTHORITIES

New Jersey Domestic Security Preparedness Act P.L. 2001, c.246 establishes a New Jersey Domestic Security Preparedness Task Force that includes the New Jersey Office of Homeland Security and Preparedness, the New Jersey National Guard, the Office of Emergency Management in the Division of State Police, among other State, county, and local organizations in order to maximize, enhance, and effectuate coordination of the disaster preparedness and recovery resources. Included in the duties of the task force is the development, implementation, and management of comprehensive responses to any terrorist attack or any other technological disaster, and the effective administration, management, and coordination of remediation and recovery actions and responses following any such attack or disaster.

Cybersecurity Incident Reporting P.L. 2023, c.19 requires all public agencies and government contractors in New Jersey to report cybersecurity incidents to the New Jersey Office of Homeland Security and Preparedness (NJOHSP) within 72 hours of reasonably believing an incident has occurred, while allowing private entities to report voluntarily. The bill directs NJOHSP to establish secure, confidential reporting mechanisms, and it ensures that submitted notifications are exempt from public records laws and most legal proceedings, though anonymized threat information may be shared to prevent future incidents and with law enforcement as appropriate. It also mandates the development of privacy procedures aligned with the federal Cybersecurity Information Sharing Act of 2015.

State of New Jersey Executive Order No. 5, signed by Governor Corzine on March 16, 2006, establishes the New Jersey Office of Homeland Security and Preparedness as the State Agency responsible for administering, coordinating, leading, and supervising New Jersey's counterterrorism and preparedness efforts. NJOHSP is led by a Director, who also acts as the State's Homeland Security Advisor and the Chair of the Domestic Security Preparedness Task Force. The Director and the NJOHSP shall be authorized to call upon the expertise and assistance of all State departments, divisions, and agencies to carry out their mission. The NJOHSP may, to the extent not inconsistent with any other law, employ, consult, and contract with private and public entities, and enter into such agreements with public and private individuals or entities as necessary to further the mission of the Office or of other offices and units that fall under the Director's supervision.

State of New Jersey Executive Order No. 178 signed by Governor Christie on May 20, 2015 establishes the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) as a component organization within the Office of Homeland Security and Preparedness that acts as the central State civilian interface authorized to coordinate cybersecurity information sharing and analysis across all levels of government, agencies, authorities, and the private sector pursuant to 6 U.S.C. § 133 et seq. The NJCCIC is authorized to draw upon the assistance of any department, office, division, or agency of this State to supply it with expertise and assistance, including information and personnel, to carry out the NJCCIC mission. The NJCCIC is composed of representatives of State entities, including the Office of Homeland Security and Preparedness, the Division of State Police, and the Office of Information Technology.

State of New Jersey Technology Circular 17-00-NJOIT, October 14, 2017, establishes a management structure for information security across the executive branch of New Jersey State Government including the roles and responsibilities of the Director of the Office of Homeland Security and Preparedness, the State Chief Technology Officer, the State Chief Information Security Officer, and the Director of the New Jersey Cybersecurity & Communications Integration Cell.