



**NEW JERSEY OFFICE OF  
HOMELAND SECURITY  
AND PREPAREDNESS**

**ANNUAL  
REPORT**  
STATE FISCAL YEAR  
**2022**



# ABOUT US

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) is tasked with coordinating counterterrorism, resiliency, and cybersecurity efforts across all levels of government, law enforcement, nonprofit organizations, and the private sector. Created by Executive Order in 2006 when the Office of Counterterrorism (OCT) merged with staff from the Domestic Security Preparedness Task Force (DSPTF), NJOHSP bolsters New Jersey's resources for counterterrorism, critical infrastructure protection, preparedness, training, and federal grants management.

Shortly after the tragic events of September 11, 2001, New Jersey's legislature and Governor passed and signed the Domestic Security Preparedness Act, which created the DSPTF within the Office of the Attorney General. In 2002, the Governor created the OCT by Executive Order, which remained under the Attorney General. OCT provided New Jersey with a single agency to lead and coordinate New Jersey's counterterrorism efforts with state, local, and federal authorities and with the private sector.

## MISSION

NJOHSP leads and coordinates New Jersey's counterterrorism, cybersecurity, and preparedness efforts while building resiliency throughout the State.

## CORE VALUES

**SERVICE.** We put our State and its residents first, and we put Mission before self. We take pride in being timely, agile, and relevant.

**TEAMWORK.** We stand with and behind each other. We recognize that partnerships, both internal and external, are critical to achieving success. We cannot fulfill our Mission alone.

**EXCELLENCE.** We take great pride in the quality of our work. We do every task, every project, every initiative, to the best of our ability.

**DIVERSITY.** We strive to build a workforce that is as diverse as New Jersey's citizenry. We pride ourselves on encouraging diversity of thought, perspective, and problem solving.

**INTEGRITY.** We are committed to holding ourselves accountable to the highest moral and ethical standards in our personal and professional conduct. We can be relied upon to act with honor and truthfulness.

# FOREWORD



Domestic and global threats have become a daily reality in our lives – making the headlines, dominating social media conversations, and creating unique security challenges. From mass shootings to threats against the faith-based communities to the cyber risks emerging from international events and elsewhere, we must consider their impact on local response efforts in our own backyard.

Here at the New Jersey Office of Homeland Security and Preparedness, we’re in the business of keeping people safe – a mission we carry out each and every day with every tool at our disposal. In collaboration with our partners, we recognize that current and future threats underscore the continued need for resiliency as we meet these security challenges head on. While we cannot thwart every attack, I can confidently say that our entire team is tirelessly working to mitigate risks and stands ready to respond to a potential crisis.

Key among those efforts is our “See Something, Say Something” campaign, a critical asset to our operation as NJOHSP monitors for potential threats to the public from both domestic extremists and foreign terrorist organizations. As one of our first and best lines of defense in the fight against terrorism, we continue to encourage the general public, law enforcement, first responders and private- and public-sector partners to report suspicious activity.

This past year, NJOHSP administered more than \$29 million in State and federal funding to harden security and response capabilities throughout New Jersey. In January, Governor Phil Murphy signed legislation to establish the New Jersey Nonprofit Security Grant Program. This funding has also proven to be an important State resource, especially within our faith-based communities, to supplement available federal security grants.

In the digital era, where information can be widely disseminated and easily accessible, our agency took aim at disinformation, an instrument used by bad actors to sow discord and distrust against government and law enforcement entities. In a revamped version of NJOHSP’s disinformation web portal, we have better equipped the public with the prescribed guidelines that will assist them in vetting the information they’re consuming and deciphering fact from fiction.

We continue to see a growth in our membership base for the Interfaith Advisory Council and the New Jersey Shield Program, as we look to connect our public- and private-sector partners, along with New Jersey’s houses of worship, to resources, training, grant opportunities and law enforcement personnel while igniting meaningful dialogue with various leaders and stakeholders.

This past year was marked by transitions and defined by our ability to consistently meet each moment with ingenuity, solidarity, and determination as we looked beyond the COVID-19 pandemic. The achievements forementioned and presented in this state fiscal year 2022 (SFY2022) annual report are a testament to our team of dedicated professionals who continuously strive to make New Jersey a safe place to worship, work in, visit, and call home. NJOHSP aims to utilize these different initiatives to better understand and combat the evolving threat landscape.

Sincerely,

Laurie R. Doran, Director  
December 2022

# TABLE OF CONTENTS

<b>SENIOR STAFF</b>	<b>04</b>
<b>TABLE OF ORGANIZATION</b>	<b>05</b>
<b>NOTABLE DELIVERABLES</b>	<b>06</b>
<b>COUNTERTERRORISM</b>	<b>07</b>
<b>PREPAREDNESS</b>	<b>12</b>
<b>CYBERSECURITY</b>	<b>16</b>
<b>ADMINISTRATION</b>	<b>21</b>



# SENIOR STAFF



**LAURIE R. DORAN**  
Director



**MICHAEL T. GERAGHTY**  
Acting Deputy Director, Director of NJCCIC



**RANDALL A. RICHARDSON**  
Director of Administration/CFO



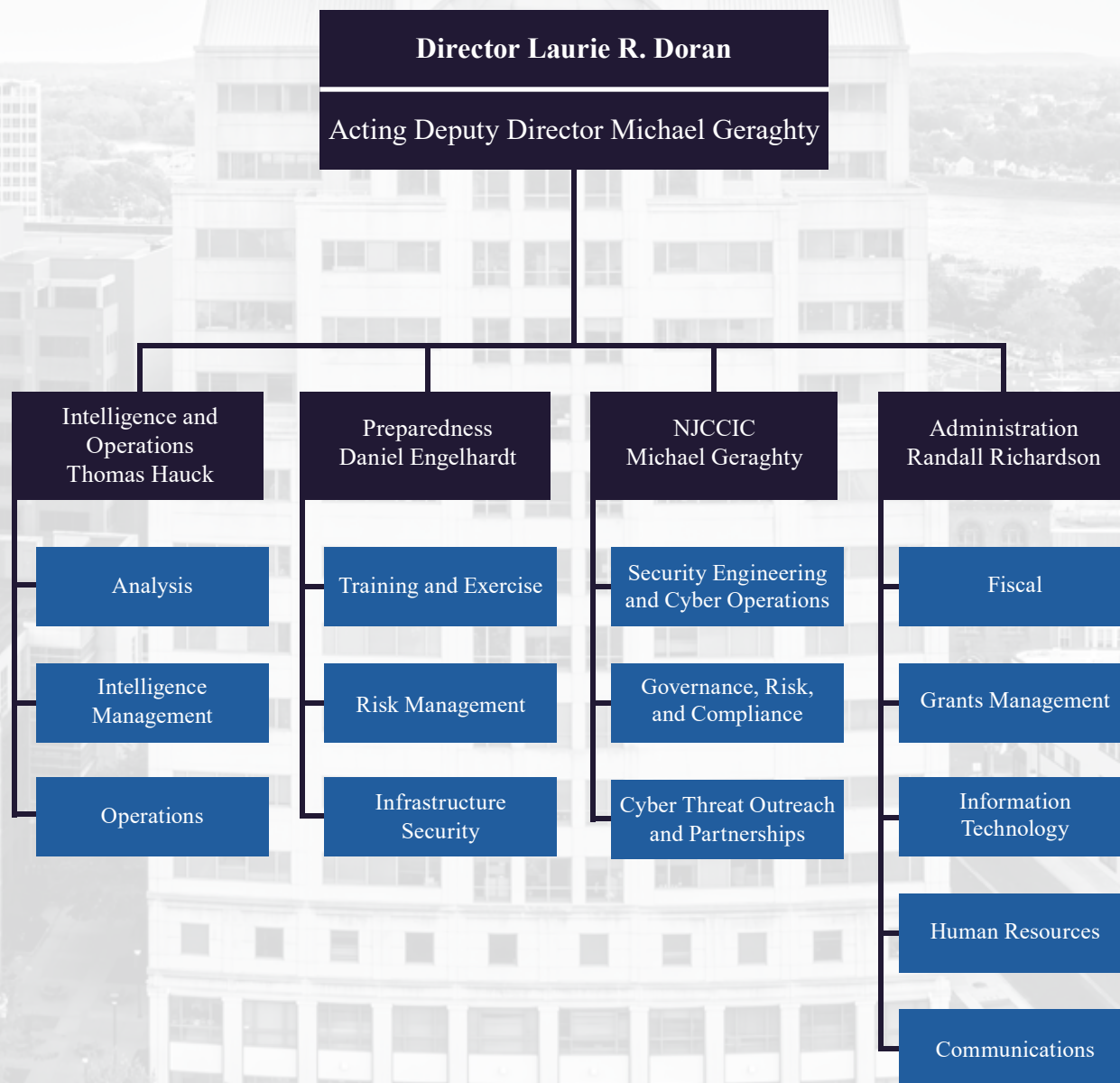
**DANIEL J. ENGLEHARDT**  
Director of Preparedness



**THOMAS G. HAUCK**  
Director of Intelligence and Operations

NJOHSP's mission is to lead and coordinate New Jersey's counterterrorism, cybersecurity, and preparedness efforts while building resiliency throughout the state.

# 2022 TABLE OF ORGANIZATION



# NOTABLE DELIVERABLES

This data includes the combined efforts of NJOHSP's four Divisions—Intelligence and Operations, Preparedness, NJCCIC, and Administration.

CATEGORY	FY22	FY21	FY20	FY19
Written Publications	721	832	754	1,012
Recipients of NJOHSP Publications	82,150	82,647	79,960	85,473
In-Person Training and Exercises Delivered	240	187	767	652
NJ Learn Online Training Completions <sup>a</sup>	350,495	226,614	179,050	106,834
Critical Infrastructure Assessments	36	75	34	52
NJCCIC Membership	12,246	11,213	10,000	9,434
Webinars and Podcasts	25	0	17	22
Website Visitors	321,032	168,782	264,047	320,000
NJOHSP Social Media Followers: Facebook, Twitter, Instagram, and LinkedIn	49,223	42,817	39,728	40,225
Interfaith Advisory Council Membership	4,099	4,052	3,817	3,431

#### Footnotes

NJ Learn<sup>a</sup> is an NJOHSP-managed Learning Management System that develops and presents critical online training for sworn law enforcement and first responders in New Jersey.

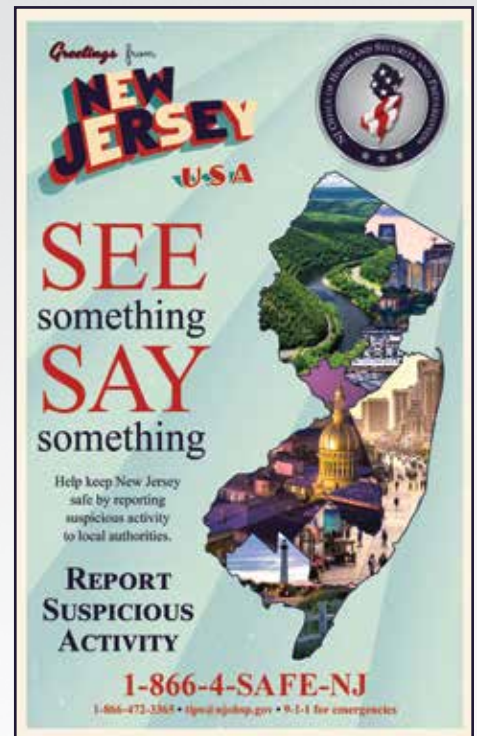
# COUNTERTERRORISM

## INTELLIGENCE MANAGEMENT BUREAU

The **Intelligence Management Bureau** (IMB) provides tailored information and intelligence to New Jersey’s law enforcement and public- and private-sector partners through regular engagement with the intelligence community and information sharing that meets State and national intelligence priorities. IMB manages statewide suspicious activity reports (SARs) while collaborating with the New Jersey Regional Operations and Intelligence Center (NJ ROIC) and other law enforcement agencies to gather, process, and share SARs in an accurate and timely manner.

### NEW JERSEY SUSPICIOUS ACTIVITY REPORTING (SAR) PROGRAM:

- NJOHSP encourages law enforcement, first responders, and private- and public-sector partners to report terrorism-related suspicious activity. The “*See Something, Say Something*” campaign benefits families, neighborhoods, and communities by bringing suspicious behavior to the attention of law enforcement. Reporting suspicious behavior could potentially stop the next terrorist incident. Even if you think your observation is not important, it may be a piece of a larger puzzle.
- NJOHSP manages the New Jersey Suspicious Activity Reporting System (NJSARS) which shares terrorism-related suspicious activity information to law enforcement partners throughout the state. NJSARS is linked to the FBI’s national SAR system, known as eGuardian, which partners with the Nationwide SAR Initiative to form a single repository accessible to thousands of law enforcement officers and analysts throughout the United States.
- To report terrorism-related suspicious activity in New Jersey and for more details on NJOHSP’s SAR program, visit [njohsp.gov/njsars](http://njohsp.gov/njsars).



### JOINT EFFORTS/REPORTS/OUTREACH/BRIEFINGS:

- IMB continues to leverage important partnerships with federal, State, county, and local agencies, as well as private-sector partners, to provide products, training, and resources. IMB developed nearly 130 SAR/intelligence reports and delivered over 80 SAR/intelligence briefings to over 5,300 external stakeholders.

## PRODUCTS AND BRIEFINGS STATISTICS

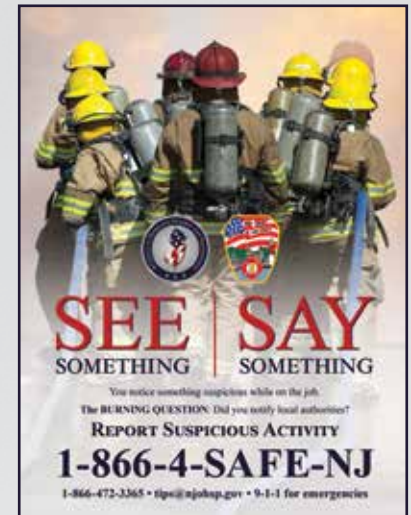
YEAR		TOTAL
SFY2022	SAR & Intelligence Briefings	84
	SAR & Intelligence-Related Products	127

## DIVISION OF FIRE SAFETY PARTNERSHIP

IMB collaborated with the New Jersey Division of Fire Safety (NJDFS) to train fire service personnel on recognizing extremist indicators and reporting suspicious activity. Select fire service personnel also received training on conducting their own fire service-related SAR briefings. IMB and Communications staff also partnered with NJDFS to create a joint “See Something, Say Something” poster for the fire service.

### “SEE SOMETHING, SAY SOMETHING” MARKETING CAMPAIGN

- IMB and Communications staff created and distributed new “See Something, Say Something” posters, materials, and public service announcements (PSA). The materials highlight the importance of reporting suspicious activity and are geared toward schools, religious facilities, and commercial private-sector industries.
- IMB joined New Jersey Shield representatives in regularly updating the various critical infrastructure sectors on suspicious activity reporting. Private sector partners continue to receive regular briefings on the campaign and the importance of contributing to NJSARS.



## NEW INITIATIVE – BEHAVIORAL THREAT ASSESSMENT MANAGEMENT (BTAM) TEAM

Behavioral threat assessment and management teams play a key role in public safety, providing expertise and experience to help better understand the level of risk when violence is feared and to develop tailored intervention methods. IMB, along with the FBI, New Jersey State Police (NJSP), New Jersey Department of Education (NJDOE), and New Jersey Department of Human Services, is coordinating the New Jersey Behavioral Threat Assessment and Management Initiative to recognize and respond to incidents of potential targeted violence, predominantly in school settings. The multi-disciplinary collaboration leverages existing processes and programs, such as NJSARS, to assist in the initial screening of reported threats and to determine if a response team should further assess and manage the situation. The team’s goal is to reduce the number of incidents that occur by creating “off-ramps” for at-risk individuals into programs for mental health or other services. Cases can be referred to NJ-BTAM through NJSARS, eGuardian, school incidents, and/or partner agency collection. NJ-BTAM also provides case consultation, assessment, and action plan support to mitigate and manage referrals, as well as providing or supporting training and education for public- and private-sector partners, including school-based threat assessment teams. IMB members have been trained by the U.S. Department of Homeland Security’s (U.S. DHS) Threat Evaluation and Reporting Course Master Trainer Program, which trains federal, state, local, tribal, and territorial homeland security partners on applying behavioral threat assessment approaches, as it relates to tips and leads, to prevent targeted violence in their areas of responsibility.

## ANALYSIS BUREAU

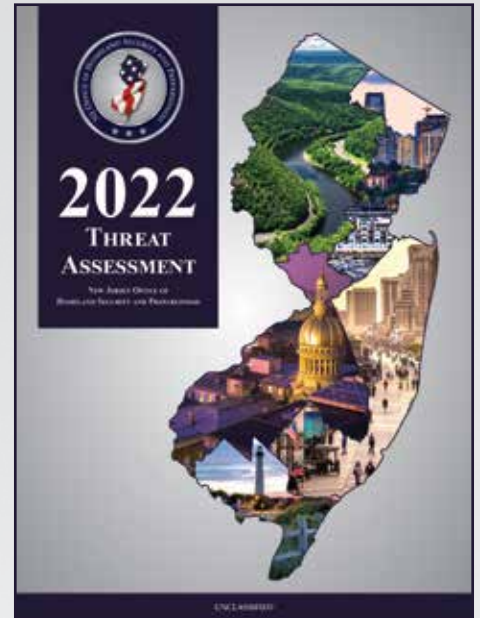
The **Analysis Bureau** provides timely, relevant, accurate, and insightful analysis regarding any threat posed by foreign terrorist organizations and domestic extremists to the State of New Jersey and the region.

In March 2022, NJOHSP released its annual threat assessment featuring detailed analysis of New Jersey's threat landscape. The assessment guided counterterrorism efforts for 2022 and provided information concerning homegrown violent extremists (HVEs), domestic extremists, foreign terrorist organizations, and cybersecurity concerns. NJOHSP forecasted that HVEs and white racially motivated extremists would continue to pose the highest threats to New Jersey. Other types of domestic extremists remained a moderate threat, while foreign terrorist organizations ranked as a low threat.

During SFY2022, the bureau increased counterintelligence (CI) production and outreach efforts to better protect New Jersey's private- and public-sector partners. As part of this effort, several Liaison Information Reports were co-authored with the FBI and distributed nationally on transnational repression and other CI concerns. NJOHSP coordinated joint meetings with the California State Threat Assessment Center and Central Florida

Exchange to strengthen and understand threats facing partner states, and initiated CI threat briefings to statewide law enforcement and military partners. As part of the 2022 Annual Threat Assessment, the bureau added a critical infrastructure protection section which sought to address various CI threats and encourage the use of strong operational security practices.

Throughout the pandemic, the Analysis Bureau provided accurate and timely products to help combat the spread of disinformation as it related to COVID-19 and other relevant national issues that affected the State. NJOHSP published these products to a newly formed, public-facing Disinformation Portal. Post pandemic, the Disinformation Portal became a permanent fixture to NJOHSP's website and continues to assist the public in identifying and vetting any truth-obscuring, manufactured information, including from nation-state actors, such as China and Russia. During SFY2022, the bureau continued to assist with State security efforts by helping provide actionable intelligence to the public and private sectors. The bureau produced multiple written intelligence assessments featured on the agency website, in addition to producing over five joint-seal products with State and federal partners, including the NJ ROIC, NJ Transit, and the FBI. The bureau also aided in the timely dissemination of intelligence via answering requests for information and by providing threat briefs discussing the annual threat assessment and relevant threat landscapes through the Hometown Security Initiative (HSI) and to PSE&G, Joint Base McGuire-Dix-Lakehurst, the Interfaith Advisory Council, the Infrastructure Advisory Committee, the Private Sector Advisory Group, the County Counterterrorism Coordinator/Joint Terrorism Task Force Executive Board, and more. NJOHSP analysts also contributed to community outreach by taking part in a faith-based town hall event, hosted by the Essex County Prosecutor's Office, that followed the attack at a synagogue in Colleyville, Texas. These efforts by the Analysis Bureau resulted in over 200 instances of intelligence-related engagements, reports, and opportunities that better enabled NJOHSP to serve the State of New Jersey.



## OPERATIONS BUREAU

The **Operations Bureau's** mission is to detect and deter terrorist activity and identify and mitigate counterintelligence (CI) threats using intelligence and law enforcement strategies.

As New Jersey has emerged from the recent pandemic lockdown, we have seen an exponential increase in public gatherings and events and with that comes a more dangerous threat landscape. Within the last year, the Operations Bureau has enhanced its capabilities to better assess and mitigate these threats.

### COUNTERINTELLIGENCE

The Operations Bureau has seen an approximate 250 percent increase in foreign delegations visiting New Jersey since the previous fiscal year. The CI Unit has conducted 154 vetting actions to determine if foreign visitors may have nefarious intentions. The bureau has provided 41 security and CI awareness briefings to New Jersey State officials traveling internationally. Members of the unit have generated or contributed to 26 CI reports, as well as 28 foreign engagement analysis products. Most recently, the CI Unit assembled a travel brief for Governor Murphy on his recent trip to Israel. This brief provided vital information to the Governor on the political landscape involving the places and officials he would be visiting. As per standard protocol, NJOHSP provides a travel brief to any New Jersey governor departing on official international business.



### COMMUNITY OUTREACH

Last year the bureau's Community Outreach team played a pivotal role in the U.S. Military's Afghan resettlement program, "Operation Allies Welcome." For six months, a member of the unit deployed to Joint Base McGuire-Dix-Lakehurst to provide language and cultural information services to both the Afghan guests and military personnel engaged in this mission. The team coordinated donations from the faith-based community and introduced local area Imams to provide religious services. The team also assisted with picnics and contracting entertainment groups to ensure a fulfilling experience for the newly arrived guests. Recognizing the cultural differences, detectives provided training and informational resource cards to local law enforcement, as well as the Afghan guests, to ensure a peaceful assimilation into American society.

In addition to the considerable amount of time and effort put forth on "Operation Allies Welcome," the outreach team coordinated quarterly meetings for the Interfaith Advisory Council, emergency conference calls in response to national and international events, provided active shooter and physical security training for houses of worship, and provided assistance to IAC members who sought to obtain nonprofit State and federal security grants.

### OPERATIONS UNIT

The Operations Unit is the bureau's outward facing public safety component. Core responsibilities include tripwire engagements, Red Team exercises,

**TRIPWIRE PROGRAM**

The Tripwire Program is an outreach initiative designed to reach private-sector merchants at hotels, malls, gun shops, and other venues. The program provides awareness of terrorism-related suspicious behaviors and encourages merchants to report suspicious activity.

**RED TEAM PROGRAM**

The Red Team Program is a tool used to test stakeholders' security through the real-time use of covert assets. The goal is to provide recommendations to address security gaps.

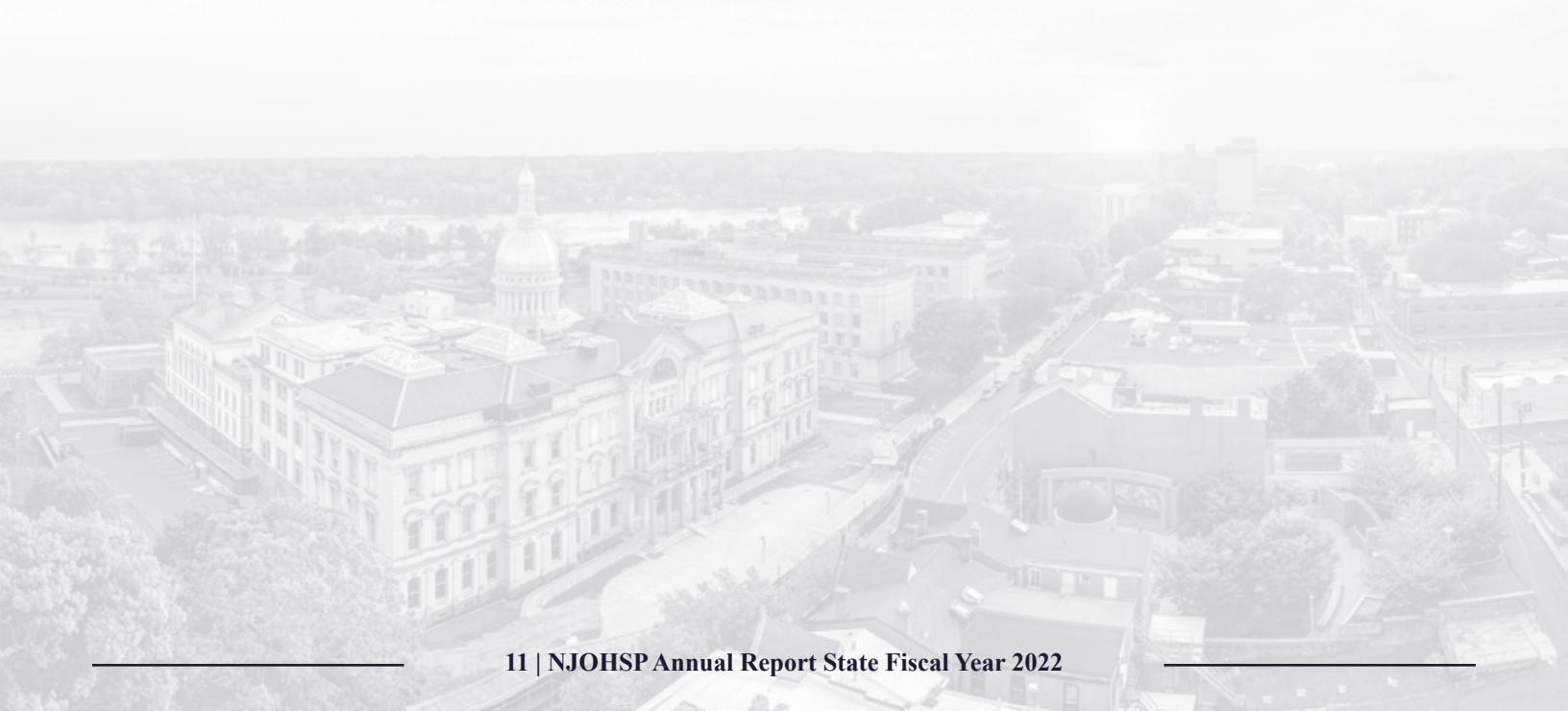
and covert hostile actor surveillance at public events, such as parades, festivals, and concerts. Last year, the team conducted 893 tripwire visits to the public and private sectors, conducted covert surveillance details on 40 mass gathering events, and directed 20 Red Team exercises throughout the state. During the summer months, the unit deployed assets to the shore communities of Atlantic, Ocean, Monmouth, and Cape May counties in support of NJOHSP's Secure the Shore initiative.

## **MILITARY LIAISON WORKING GROUP**

This year, the bureau developed and chaired a Military Liaison Working Group. This working group was born out of the "Operation Allies Welcome" program and meets quarterly, focusing on common concerns of New Jersey's law enforcement and all branches of the military operating in New Jersey. As the military has a considerable footprint in the state, the sharing of intelligence and partnered operations is vital to the safety of military personnel and those members of the public who reside near military facilities.

## **INVESTIGATIONS**

The Investigations Unit of the Operations Bureau is responsible for conducting investigations into potential terrorist activity and developing confidential relationships with members of the public. In the last year, the unit reviewed and assessed over 1,100 suspicious activity reports for threat information and conducted 32 threat mitigation investigations.



# PREPAREDNESS

## RISK MANAGEMENT BUREAU

The **Risk Management Bureau** (RMB) identifies gaps and implements programs to build and enable homeland security and preparedness capabilities across New Jersey's public and private sectors. The bureau identifies gaps through risk-informed capability assessments, partner engagement, and data analysis. Programs are implemented by leveraging partnerships, committees and working groups. Capabilities are built and enabled by sharing protective measures, risk mitigation strategies, program resources, and funding opportunities.

The bureau manages the operations of the DSPTF, Domestic Security Preparedness Planning Group, and the Infrastructure Advisory Committee, as well as the DSPTF Unmanned Aircraft System and School Security subcommittees, on behalf of the director of NJOHSP. The task force and its subcommittees focus statewide resources and identify opportunities to build a more prepared and resilient New Jersey. During SFY2022, the bureau directed the DSPTF in the assessment and prioritization of 32 Homeland Security Grant Program project applications totaling over \$12.5 million in requested federal grant funding.

The bureau developed and submitted New Jersey's Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) to the U.S. DHS. The THIRA identifies the most challenging threats, hazards, and risks to determine the level of capability needed to address those threats and hazards. The output from the THIRA lays the foundation for determining a community's capability gaps in the SPR. RMB continues to focus on outreach and diversifying its data sources in developing the report across federal, State, county, and nongovernmental homeland security and emergency management partners.

The bureau continued to organize HSI seminars. Through this initiative, the bureau coordinates with private sector organizations and local communities throughout New Jersey for the delivery of customizable in-person and virtual seminars designed to encourage audience participation and interactive discussions with government representatives on an array of topics, including: recognizing and reporting suspicious activity, active shooter preparedness, cybersecurity best practices for small businesses, physical protective measures, and individual and community preparedness. Participating agencies – such as NJOHSP, NJSP, U.S. DHS, and local police departments, offices of emergency management, and county prosecutors' offices – focus on educating community participants on common risks they may face and provide them with tools and resources to assist in enhancing security and building their preparedness posture. Over the past year, the bureau coordinated the delivery of 12 seminars to more than 1,346 people.

The New Jersey Shield Program, a collaborative effort between NJOHSP and NJ ROIC, managed by the bureau, continued to see growth. This program focuses on working with public- and private-sector organizations to build a more prepared and resilient New Jersey. The membership has grown to more than 1,300 members. The membership is comprised of individuals across three countries, 23 states, and New Jersey's 21 counties. Additionally, New Jersey Shield launched a monthly crime and suspicious activity reporting briefing. Analysts from the NJ ROIC and NJOHSP provide members with 30-day analysis on such trends as vehicle thefts, car jackings, shootings, types of suspicious activity being reported, as well as the most impacted sectors.

## INFRASTRUCTURE SECURITY BUREAU

The mission of the **Infrastructure Security Bureau (ISB)** is to strengthen the security and resiliency of New Jersey, its critical infrastructure, and its institutions by managing risks through collaborative and integrated efforts of the whole community.

Through physical security assessments and vulnerability discussions, the bureau recommended options for consideration to enhance resilience and reduce risk at these and other facilities, including houses of worship. During SFY2022, NJOHSP conducted physical security assessments for 36 facilities, including schools as well as county superintendent and board of election offices.

ISB engaged with soft target facilities, including houses of worship. It provided in-depth knowledge of the New Jersey Nonprofit Security Grant Program and the application process while reviewing facility security vulnerability concerns. The bureau coordinated with county infrastructure partners to develop a critical infrastructure questionnaire as an asset identification and verification tool in the ongoing review of infrastructure information contained within the State Asset Database.

The bureau collaborated with the New Jersey Cybersecurity and Communications Integration Cell, New Jersey Department of State's (NJDOS) Division of Elections, county infrastructure partners, and elections officials to help ensure New Jersey conducted safe and secure primary and general elections in SFY2022. As these were conducted primarily through vote-by-mail ballots, the bureau also assisted in securing elections drop boxes and processes.

The bureau continues to facilitate the Critical Infrastructure Review Team, which is comprised of federal, State, and local partners. The team shares information, discusses state- and local-level assets, recognizes common vulnerabilities, and recommends vulnerability assessment best practice strategies for stakeholders.

The bureau coordinated with federal, State, and county critical infrastructure partners to continue promoting and sharing:

- Resources on protection, mitigation, and resiliency
- Relevant training on mitigation measures for ransomware threats and industrial control systems through stakeholder outreach, including HSI seminars
- Virtual stakeholder engagements and subsector working group meetings, as well as the facilitation of Critical Infrastructure Review Team meetings

In collaboration with the NJSP Infrastructure Protection Unit, ISB developed an updated Facility Self-Assessment Tool that serves as a security best practices resource to assist small businesses and organizations in becoming more resilient and to better secure their operations and personnel.



# TRAINING AND EXERCISE BUREAU

The mission of the **Training and Exercise Bureau (TEB)** is to strengthen capabilities across the State to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose a high risk. The bureau is responsible for developing, administering, and coordinating training and exercises for homeland security stakeholders in cooperation with federal, State, local, and private-sector partners.

## BUREAU HIGHLIGHTS FOR STATE FISCAL YEAR 2022

The bureau continues its expansion to facilitate cybersecurity training for public and private-sector partners through the National Cybersecurity Preparedness Consortium and the Regional Intelligence Academy (RIA), a training partnership between NJOHSP, the NJSP, and the Jersey City-Newark Urban Area Security Initiative, often referred to as UASI.

### NJ Learn

NJOHSP manages the NJ Learn online learning management system for New Jersey first responders, which also requires continual upgrades, revisions, and expansion to meet the growing need and desire for web-based training. Management involves 164,000 learner accounts with transcripts and the development of courseware and resources for 24/7 delivery. The COVID-19 pandemic emphasized the need for online learning, and NJ Learn played a critical role in supporting the agency’s training and exercise initiatives by using web-based courses to supplement in-person learning.

### EXERCISE UNIT

The Exercise Unit and Port Authority of New York and New Jersey conduct monthly meetings with a national group of ports and transportation carriers regarding the safe transportation of electric vehicles equipped with lithium-ion batteries. This coordination helps identify critical training and exercise gaps. The Exercise Unit also conducted multiple exercises for bi-State rail barge employees in response to various emergencies and conducted a full range of exercises with the New Jersey Institute of Technology regarding active shooter and fentanyl overdose mass casualty incidents.

### TRAINING INITIATIVES

TEB assisted with the redesign and redevelopment of online courseware for the NJSARS user training course. The bureau continues to support and collaborate with the New Jersey Office of the Attorney General (NJOAG) and the New Jersey Division of Criminal Justice to develop courseware and resources for law enforcement elective and mandatory training. Courseware development focuses on directives for law enforcement and the NJOAG’s Community Law Enforcement Affirmative Relations Institute.

NJ LEARN AND EXERCISE SUPPORT UNIT SFY2022 STATISTICS	
NJ Learn	
Active Course Enrollments	418,589
Online Training Completions	350,495
Instructor-Led Completions	634
Total Training Completions	355,569
Total New Users	5,627
New Online Courses	47
EXERCISE SUPPORT UNIT	
Exercises Collaborated and Coordinated by NJOHSP	18
Exercise Participants	473



## ACTIVE SHOOTER RESPONSE TRAINING PROGRAM

The Active Shooter Response Training Program provides overall awareness of behavioral indicators, potential attack methods, and the actions that may be taken when confronted by an active shooter. This training offers guidance on how to prepare for and respond to an active shooter event based on the U.S. DHS “Run. Hide. Fight.” concept. During SFY2022, 884 people from both the public and private sector participated in the program.



## HOUSES OF WORSHIP SECURITY PROGRAM

The Houses of Worship Security Program is designed to reach faith-based communities and provide strategies to increase security and preparedness in and around their facilities. This program was delivered to more than 500 parishioners at religious facilities between July 2021 and June 2022.

## TRAINING BRANCH EXTENDS RIA REACH

NJOHSP continued to play a critical role in supporting RIA initiatives with training development, course revisions, and allowable in-person deliveries, as well as collaboration with live virtual training to provide web-based courses to supplement in-person learning.

In collaboration with the New Jersey Office of Emergency Management (NJOEM) and the NJ ROIC, TEB created a new Field Intelligence Officer Training curriculum, and completed a 10-day in-person pilot program. The program focuses on training full-time NJOEM employees assigned to the NJ ROIC.

To accommodate in-person training restrictions, NJOHSP and the RIA coordinated with the National White Collar Crime Center for seven virtual live training deliveries during the SFY2022. Approximately 383 attendees completed these intelligence trainings.

Continued expansion in training development and course completion numbers demonstrate that TEB, with the help of its partners and other State agencies, has a significant impact on providing valuable mission-critical training that will strengthen first responders’ capabilities.

<b>RIA AND NJOHSP SFY2022 TRAINING STATISTICS</b>			
<b>REGIONAL INTELLIGENCE ACADEMY</b>			
<b>Participants Trained</b>	<b>443</b>	<b>Programs Delivered</b>	<b>9</b>
<b>TERRORISM AWARENESS AND PREVENTION</b>			
<b>Participants Trained</b>	<b>27</b>	<b>Programs Delivered</b>	<b>2</b>
<b>COUNTERTERRORISM AWARENESS FOR LAW ENFORCEMENT</b>			
<b>Participants Trained</b>	<b>427</b>	<b>Programs Delivered</b>	<b>10</b>
<b>Participants Trained via e-Learning</b>	<b>152</b>	<b>E-Learn Deliveries</b>	<b>1</b>
<b>ACTIVE SHOOTER INITIATIVE</b>			
<b>Participants Trained</b>	<b>1,294</b>	<b>Programs Delivered</b>	<b>30</b>

# CYBERSECURITY

## NEW JERSEY CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

The mission of the **New Jersey Cybersecurity and Communications Integration Cell** (NJCCIC) is to lead and coordinate New Jersey’s cybersecurity efforts while building resiliency to cyber threats throughout the State. In this capacity, the NJCCIC is tasked with the strategic development and execution of the State’s cybersecurity efforts, which include acting as the State’s one-stop-shop for cybersecurity information sharing, threat intelligence, best practices, and incident reporting and response. In addition, the NJCCIC develops, manages, and executes an information security program that ensures the confidentiality, integrity, and availability of information resources, systems, and services for the State of New Jersey Executive Branch’s departments and agencies.

Located at NJ ROIC, the NJCCIC acts in a cyber fusion center capacity and is comprised of staff from NJOHSP, the New Jersey Office of Information Technology (NJOIT), and the NJSP. The NJCCIC also maintains partnerships with other State and federal agencies, including the NJOAG; the FBI; the U.S. DHS's Cybersecurity and Infrastructure Security Agency (CISA); national organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), Health Information Sharing and Analysis Center, Financial Services Information Sharing and Analysis Center, Electricity Information Sharing and Analysis Center, and Elections Infrastructure Information Sharing and Analysis Center; and private-sector organizations and operators of critical infrastructure and key resources throughout New Jersey and beyond.

The overall impact and establishment of the NJCCIC as an essential cybersecurity resource for New Jersey and elsewhere was borne out by its continued growth and effectiveness in meeting its mission goals and objectives. In SFY2022, membership grew by 1,033 for a total of 12,246 members. Its following includes members from 45 states, three territories, and 50 countries around the world. Members receive the NJCCIC’s cyber threat intelligence products, alerts, advisories, training notifications, and other cybersecurity products and services.

Staff responded to or assisted in 579 cybersecurity incidents reported to the NJCCIC in SFY2022. Of those incidents, 34 were for ransomware infections impacting New Jersey public- and private-sector organizations and private citizens. As ransomware attacks increase in sophistication and result in significant disruptions to impacted organizations’ operations with high remediation costs, the NJCCIC continues to collaborate with its partners to provide risk mitigation strategies and response services. In addition to its Ransomware Mitigation Guide, the NJCCIC maintains profiles on hundreds of ransomware variants and provides members with updates to the tactics and techniques that ransomware threat actors use.



### THE THREAT LANDSCAPE

Email-based attacks remain the most prevalent, persistent, and effective cybersecurity threat affecting New Jersey and organizations around the world. A significant number of incidents the NJCCIC responds to begin with a victim receiving a targeted email message containing prompts to open malicious attachments, click links, or

divulge sensitive information. Threat actors often use email attacks to gain a foothold in an organization's network by compromising a legitimate user's credentials or executing malware on the recipient's systems. Email-based attacks are so prevalent because convincing a person to take a desired action is typically easier than hacking into a system.

During any given month, NJCCIC-managed enterprise email content filters have blocked over half of all emails sent to New Jersey State government departments and agencies, as the inbound messages contained malicious attachments, links, or phishing content or were determined to be spam. In SFY2022, the NJCCIC's filters blocked more than 429 million emails intended for New Jersey State government workers, with over 323,000 emails deemed targeted threats.

In addition to the State's email content filtering systems, the NJCCIC also manages the State's intrusion detection and prevention systems and other enterprise technologies that provide network, endpoint, application, and data protection. These technologies were used to analyze and block more than a million internet-based attacks from around the globe, with almost 34 million targeting the State's public-facing web applications.

The NJCCIC increased efforts to identify and remove phishing websites impersonating multiple New Jersey state agencies with the intent to steal user credentials and personally identifiable information, such as Social Security numbers and driver license numbers. By submitting cease-and-desist requests for the removal of these websites, the NJCCIC potentially prevented New Jersey residents from having their information stolen, which could lead to account compromises, identity theft, and subsequent malicious cyber activity.

## CAPABILITY BUILDING

The purpose of the NJCCIC providing near real-time threat intelligence, cybersecurity information, and best practices is to ensure individuals and organizations are aware of threats and have the information necessary to mitigate risks associated with them. In doing so, the NJCCIC develops a better overall cybersecurity posture for the State while increasing its capabilities in preventing and responding to cyber threats.

The NJCCIC distributed 267 cybersecurity products in state fiscal year 2021 and 281 in SFY2022. Of the 548 cybersecurity products distributed, 36 were cybersecurity alerts, 349 were cybersecurity advisories, and the remaining were weekly and monthly bulletins and training announcements. In addition to distributed products, the NJCCIC published new threat profiles; best practices documents; updates on current and emerging cyber threats, including phishing and other social engineering threats; and cyber risk mitigation strategies and tactics to its website. The NJCCIC's body of work is available at [cyber.nj.gov](https://cyber.nj.gov), which intends to assist businesses, organizations, and private citizens in bolstering their cybersecurity capabilities and defending against cyber threats, thereby becoming more resilient to cyberattacks.

The NJCCIC also coordinated and provided cybersecurity awareness training across Executive Branch departments and agencies during the past two fiscal years. NJCCIC staff delivered over 113 external cybersecurity threat briefings and presentations to roughly 6,000 individuals across the state, despite limitations due to the COVID-19 pandemic. In addition, the NJCCIC hosted nine instructor-led advanced cybersecurity training classes for 353 cyber defenders and investigators, covering such topics as intrusion detection, cyber incident response, computer forensics, and cybersecurity analysis.



In state fiscal year 2020, the NJCCIC began an initiative to notify New Jersey State agencies, county and local governments, law enforcement agencies, educational facilities, and healthcare organizations of users whose account credentials were posted, shared, for sale, or sold on various dark web forums, markets, and paste sites. Threat actors likely obtained these credentials as a result of data breaches or malware infections. The intent of this program is to mitigate the risk of account compromises that could lead to unauthorized access of accounts and network assets, as well as identity theft and other fraudulent activities. During SFY2022, the NJCCIC notified affected entities of 7,124 exposed credentials.

In late SFY2022, the NJCCIC began offering a cyber range platform to State, county, and local government and higher education cybersecurity personnel. The goal of the cyber range is to assist personnel in developing information technology and cybersecurity skills, as well as to exercise their cybersecurity incident response capabilities. In SFY2022, 23 cyber range incident response exercises were conducted.

The NJCCIC also entered a new partnership with several other states to form a Joint Cybersecurity Operations Center consisting of intelligence analysts, cybersecurity engineers, and information security professionals. The goal of the partnership is to open communication between the states in order to share knowledge, methodologies, cyber threat information and indicators, and best practices.

In August 2021, the NJCCIC organized and hosted the virtual symposium, “Achieving Cyber Resilience: Best Practices & Free Resources for New Jersey Public Sector Partners,” which provided public-sector partners with information on cybersecurity best practices and featured presentations from the NJCCIC, CISA, and MS-ISAC on the no-cost resources available via their respective organizations. Additionally, NJOHSP provided New Jersey public-sector agencies with information related to cybersecurity grant opportunities, which the Grants Management Bureau administers.

The NJCCIC utilizes its website and social media channels to provide the public awareness of emerging trends, threats, and analysis, in addition to current events, conferences, and training opportunities. In SFY2022, the NJCCIC website had 150,000 visitors and 250,000 page views. In addition, the NJCCIC published 900 social media posts and gained 1,300 new followers. The NJCCIC member portal, which provides more targeted information, increased handling-level products, and archive functionality of products for vetted individuals, added 137 members.

## **STEM OUTREACH**

In 2022, the NJCCIC supported the strong placement of New Jersey high school students in the CyberStart America competition, with the State totaling the highest number of finalists, and National Cyber Scholars in the nation, which amounted to 274 and 124 respectively. The latter statistic nearly doubled, having increased from 63 scholars awarded to New Jersey students in 2021. There are several pathways to qualify for the next National Cyber Scholarship competition, including CyberStart America, a free online NJCCIC-promoted program that helps students discover their interest in cybersecurity and develop their talent and skills. The number of participants increased greatly to 3,894 total registered students, beating last year’s then-record-breaking turnout of 2,188. These students attempted various computer security puzzles and challenges that assessed their skills in areas such as password cracking, reverse engineering, memory corruption, and cryptography.

In addition, 18 New Jersey high school students were named Cyber Ambassadors in 2022. These students recruited over 300 of their peers to join them in participating in the 2022 CyberStart America program. As student advocates of cybersecurity, their teamwork inspired other young minds to explore their interests in this field.

The NJCCIC's outreach into the K-12 STEM community in New Jersey continues along with efforts to partner with the State's colleges and universities. NJCCIC representatives act as members of NJDOE's Computer Science Advisory Board that is developing K-12 computer science curriculum requirements. They also participate on cybersecurity advisory boards for several state universities and colleges. The NJCCIC has developed a robust internship program that was extended to high school students this past year. Over the past four years, the NJCCIC has hired 15 of its interns as full- or part-time employees, providing a pathway for students to gain experience in the cybersecurity field that eventually results in career opportunities.

In state fiscal year 2022, the NJCCIC sponsored and assisted in the development of the JerseyCTF, a cybersecurity capture-the-flag competition and conference that aims to inspire interest in the field of cybersecurity. Conference speakers included cybersecurity professionals from the NJCCIC, private-sector organizations, and federal government agencies. Event participation reached 1,466 students from all over the world.

## **RISK MANAGEMENT**

In 2021, the NJCCIC continued expanding its risk management services by assisting other agencies with conducting cybersecurity risk assessments of four high-profile statewide systems. The NJCCIC, in coordination with NJOIT's system architecture review process, reviews all systems being implemented on the Garden State Network for compliance with the Statewide Information Security Manual. The NJCCIC also performs system security reviews of potential and existing third-party vendor partners undergoing purchasing reviews and requests for proposals.

The NJCCIC continued to implement the Statewide Cyber Threat Grid in which intrusion detection sensors will be placed at the perimeter of each of New Jersey's 21 county networks and the two New Jersey UASI cities, as well as the perimeter of the State government network. The purpose of this project is to provide increased protection for county and State government networks, systems, and information; increased situational awareness of threats that can potentially impact the security of county and State government networks and systems; increased capability to respond to threats in a more timely and effective manner; and the ability to correlate alerts, trends, and analytics across multiple networks. This creates a New Jersey Statewide Threat Grid. As of June 2022, 25 sensors were installed, including the first cloud sensor pilot installation.

## **ON THE ELECTION FRONT**

The NJCCIC continued to partner with the NJDOS's Division of Elections and county elections officials throughout SFY2022 to provide security for elections systems and processes. Cybersecurity critical infrastructure analysts are embedded within the NJDOS's Division of Elections' office to assist with the security of New Jersey's elections systems. The analysts are responsible for coordinating all cybersecurity efforts related to the elections systems. This includes support for the Division of Elections' continuity of operations plan (COOP) and ensuring the statewide voter registration system is secure.

Throughout SFY2022, the NJCCIC continued outreach and coordination efforts with federal, State, and local elections officials and security partners to maintain communications and planning for the primary and midterm elections. An Election Day situation room at the NJCCIC was activated on primary election day. In coordination with federal, State, and local agencies, the team used multiple synchronized platforms to monitor and report on election day security. This outreach continued into the 2022 midterm election cycle.

In the last several years, the NJCCIC assisted all 21 county partners with establishing their COOPs to manage the election in each county and worked with them throughout SFY2022 to update these plans. The purpose of the reviews was to document emergency response and continuity of operations capabilities in the event of a range of physical and cybersecurity incident scenarios that could impact the effective and efficient conduct of elections in New Jersey.

## NJCCIC STRATEGIC PLAN

In September 2020, the DSPTF ratified the NJCCIC's 2021-2025 cybersecurity strategic plan. The plan represents a pathway to achieve improved cyber resilience through a series of interrelated strategic goals and action items intended to help safeguard New Jersey's institutions, businesses, and individuals. It includes broad statewide goals applicable to all public- and private-sector institutions and individuals, as well as those specific to the Executive Branch of the New Jersey State government, for which the NJCCIC has direct oversight. This strategic plan also supports the overall mission of NJOHSP, whereby cybersecurity is woven into its counterterrorism, counterintelligence, and preparedness functions.

## NJCCIC STRATEGIC GOALS

- **Strategic Goal 1 - Cybersecurity Leadership:** Lead and coordinate a whole-of-state approach to cybersecurity.
- **Strategic Goal 2 - Capability Building:** Increase the security posture and resilience of public and private institutions, critical infrastructure assets and key resources, and the residents of New Jersey by building cybersecurity capabilities.
- **Strategic Goal 3 - Partnerships and Collaboration:** Cultivate strategic partnerships and pervasively collaborate with public- and private-sector organizations to increase the capacity and capability to recognize threats and defend against and respond to cyberattacks perpetrated against the citizens, public and private institutions, and critical infrastructure of New Jersey and the United States.

# ADMINISTRATION

## FISCAL BUREAU

The **Fiscal Bureau** is focused on the effective management of NJOHSP's \$12.8 million State operations budget, \$11.5 million cybersecurity budget, and approximately \$121 million of administered State and federal grant funds.

The fiscal team supports the Grants Management Bureau by processing grant reimbursement packages and maintaining financial records within the New Jersey Comprehensive Financial System. In SYF2022, the financial team processed over \$40 million in State and federal grant expenditures.

## NJCCIC SUPPORT

The Fiscal Bureau supported the efforts of the NJCCIC, which is in its sixth year as the lead agency responsible for securing New Jersey's cyber technologies and network from malicious attacks, by working in tandem with the NJCCIC Deputy Chief Information Security Officer. The bureau implemented a cybersecurity reimbursement initiative of more than \$3 million for the Executive Branch with 100 percent program compliance for the third successive year. The financial team procured over \$10 million of cybersecurity-related products and services to protect the Garden State Network and New Jersey's cyber infrastructure from malicious acts. The Fiscal Bureau and the NJCCIC improved external procurement processes and developed a cohesive system to benefit the Executive Branch.

## PASSAIC VALLEY WATER RESPONSE

In September 2021, the Fiscal Bureau managed a coordinated response to the water crisis faced by residents receiving water from the Passaic Valley Water Commission, which serves the Northern communities of Patterson, Clifton, and Passaic. While the commission pumps over 145 million gallons of water per day, a tragic storm caused the pumping stations to fail. NJOHSP immediately responded and provided over 65 pallets of potable water for residents in need. Additionally, NJOHSP provided 800 blankets for residents, as well as emergency food rations.



NJOHSP worked in collaboration with the NJOEM, along with the New Jersey National Guard, to secure delivery of needed commodities.

## BLANKET DISTRIBUTION

During SFY2022, NJOHSP collaborated with the New Jersey Department of Human Services (NJDHS) and successfully distributed 15,000 blankets to county shelters from State stockpiles. With the assistance of NJDHS, the Fiscal Bureau ensured that the appropriate counties received the blankets. NJOHSP also collaborated with the New Jersey Department of Agriculture to distribute animal crates from the State stockpile to multiple counties in New Jersey. Fiscal monitored all deliveries, coordinating with and ensuring that agencies received the proper equipment.

## SINGLE AUDIT

NJOHSP has secured a 100 percent clear audit for the third year in a row during its single audit examination. This is a significant accomplishment and the fiscal team prides itself on integrity and solid taxpayer service. The bureau's motto is "Integrity is doing the right thing even when no one is looking."

## GRANTS MANAGEMENT BUREAU

The **Grants Management Bureau (GMB)** is charged with the efficient and effective management and administration of federal and State homeland security grant funding. Grant funding enables New Jersey to enhance its capabilities to prevent, protect, mitigate, respond to, and recover from acts of terrorism and other catastrophic events.

As NJOHSP is the designated State Administrative Agency for homeland security grants, GMB initiates an intense, comprehensive strategic planning process – engaging hundreds of State, county and municipal subject matter experts to identify vulnerabilities and prioritize projects to receive funding to close security gaps. GMB currently manages over \$151 million of open federal/State grants that improve upon New Jersey's preparedness and security posture.

## URBAN AREA SECURITY INITIATIVE (UASI)

The Jersey City-Newark UASI includes Jersey City and the City of Newark, as well as the counties of Bergen, Essex, Hudson, Middlesex, Morris, Passaic, and Union. First responder disciplines work with State, county and municipal units of government to collaboratively enhance counterterrorism capabilities and planning for and responding to catastrophic events within and across geographic boundaries. During the federal fiscal year 2022 (FFY2022) grant cycle, the GMB awarded \$18,915,000. UASI funds enhance New Jersey's preparedness and security measures within this region of the state.

## STATE HOMELAND SECURITY PROGRAM (SHSP)

NJOHSP utilizes a risk-based formula to distribute local share funding among New Jersey's 21 counties. Grant funds must support terrorism preparedness by building, enhancing, or maintaining capabilities that relate to prevention, protection, mitigation, response, or recovery. Twenty-five percent of the funds are allocated to support counterterrorism and law enforcement operations. During the FFY2022 grant cycle, the GMB awarded \$7,074,841. SHSP funds enhance New Jersey's preparedness and security measures statewide.

## NONPROFIT SECURITY GRANT PROGRAM (NSGP) - STATE AND FEDERAL

The NSGP is a competitive program that awards funding to registered nonprofit organizations, as defined under section 501 (c)(3) of the Internal Revenue Code of 1986, at high risk of terrorist attack. NJOHSP administers both the federal and State NSGP programs. Eligible organizations may apply for funding to purchase and install security equipment and/or provide security personnel on their owned or leased property. Awards are based upon State and federal investment application reviews and recommendations.

In 2022, the GMB awarded over \$19 million dollars of federal Nonprofit Security Grant Program funding to 131 recipients. NJOHSP also awarded over \$2.7 million dollars of New Jersey Nonprofit Security Grant Program funding. Of that amount, \$530,000 was awarded to 53 recipients to fund security personnel and over \$2.22 million was awarded to 42 recipients to fund target-hardening equipment. GMB anticipates awarding an additional \$5 million to eligible nonprofit organizations facing the greatest risk of a terrorist attack during the state fiscal year 2023 (SFY2023) grant cycle.

## OTHER ACCOMPLISHMENTS

GMB staff conducted 39 compliance monitor reviews, each of which are designed to ensure proper adherence to both financial and programmatic grant regulations and requirements.

GMB is building out a business framework for the New Jersey Reproductive Health Security Grant Program, which will consist of \$5 million for those healthcare service providers that face the risk of violence, vandalism, harassment, threat, attacks and other unlawful activities.

GMB is also applying for and anticipates receiving over \$3.4 million for the first year of the federal, State and Local Cybersecurity Grant Program. This program will provide additional funding in out-year grant cycles.

## INFORMATION TECHNOLOGY BUREAU

The **Information Technology Bureau** provides NJOHSP with secure, innovative, and reliable technology-based services. In this fiscal year, the bureau accomplished several major milestones:

The bureau prioritized support to NJOHSP staff returning to the workplace and provided a seamless transition with regards to technology whether teleworking or being at the physical office. To simplify this process, the bureau began the process of transitioning to a remote-capable phone system so wherever an employee is located, they can connect with staff and external stakeholders through multiple communication methods. The team anticipates the completion of this implementation within the next fiscal year.



The bureau also fully completed upgrades from end-of-life hardware and operating systems to fully supported systems. This included multiple critical applications with minimal downtime. The team is testing internal multifactor authentication procedures to access critical systems. This will further harden security and provide greater visibility into auditing any suspicious activities.

In coordination with NJOIT, the bureau developed a migration plan to migrate server infrastructure and applications into the primary datacenter. This allows for a level of geographic redundancy not previously enjoyed and brings NJOHSP into compliance with Executive Order 225 for information technology consolidation.

## HUMAN RESOURCES BUREAU

The **Human Resources Bureau** is charged with maximizing organizational and individual potential while facilitating a work-life balance accomplished through recruitment of top talent, workforce training and development, retention of high-performing workforce and ensuring compliance with State and federal employment laws. The bureau houses NJOHSP's facilities management function.

NJOHSP was aggressive in filling vacancies, as well filling newly created positions from the expansion of the NJCCIC. NJOHSP onboarded 19 new hires during this fiscal year. Although these new hires do not account for the vacancies which occurred during this same fiscal year, the net result was even. NJOHSP anticipates returning to full capacity and onboarding new hires during SFY2023.

The COVID-19 pandemic brought a historic change to the public-sector workplace with the introduction of teleworking, a newly introduced option for the State government workforce. From 2020 to 2022, for the first time ever, NJOHSP staff worked remotely under the Public Health Emergency declared in Executive Order 103 (2020). For NJOHSP, largely due to the technology and the type of work being done, close to 90 percent of its workforce was able to work remotely. The only exception was employees assigned to NJOHSP's Counterterrorism Watch Desk, which has a 24/7 in-person operation managing NJSARS.



In 2022, the Civil Service Commission established a pilot program to provide for a model telework program for State employees, launched on July 1, 2022, and running for a period of one year. (See In the Matter of Model Telework Pilot Program, State Executive Branch Employees, CSC Docket No. 2022-2243). Under this program, certain eligible employees may telework for up to two days per calendar week.

As the entire nation recovers from the COVID-19 pandemic, NJOHSP's operation has indefinitely changed and the latest technology allows it to remain viable and effective.

## COMMUNICATIONS

The **Office of Communications** strives to extend NJOHSP's messaging, initiatives, and programming. It relies on a variety of modern and time-tested tools to reach targeted audiences, ranging from partners to the media to the broader public.

In SFY2022 and in support of the organization's overall mission, the Communications staff were able to reach a significantly larger audience than the year prior, showing increased impressions across all platforms through strategic outreach, both to the public and the media.

The office's social media accounts—Twitter, Facebook, Instagram, and LinkedIn—experienced a notable upswing in audience growth with a combined count of more than 60,000 NJOHSP and NJCCIC followers – a 20% upsurge from the previous year, with Twitter sustaining the largest influx of followers. Over the course of SFY2022, topics central to NJOHSP's social media posts focused on statewide preparedness, counterterrorism and cybersecurity efforts, activities, and milestones.

Communications relaunched the monthly "Intelligence. Unclassified." podcast in early April, adding video formatting to its production elements. Additionally, staff produced and debuted a new, weekly "Terrorism At a Glance" podcast, featuring rotating in-house presenters covering a snapshot of recent terrorism-related news from around the world, including right here in New Jersey. These podcasts average a combined monthly listener base of at least 500.

The team responded promptly with targeted communications in response to unfolding and ongoing current events, like the incident that transpired in New York City this past April, when an accused New York City shooter who had ties to New Jersey allegedly opened fire in the subway. Press releases drafted and distributed during this time frame touched on a variety of subject matter, including safe drone usage, cybersecurity campaigns, grant opportunities, threat assessments and more.

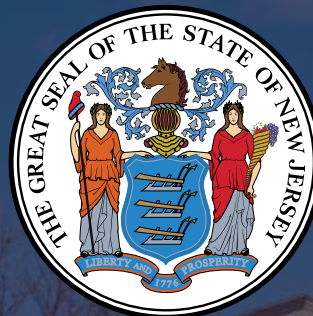
As one of NJOHSP's most prominent assets, its websites kept visitors apprised of consistent updates regarding law enforcement and homeland security initiatives throughout the region. Website analytics logged over 171,000

unique visitors to the site. The NJOHSP websites cover all scopes of the operation, including intelligence reports, trainings and exercises, cybersecurity trends and best practices, membership programs, along with all other relevant information.

The office worked in close collaboration with leadership to identify and create opportunities to promote NJOHSP's mission, accomplishments, resources, and partnerships. This coordination led to impactful interviews between media and senior staff, as well as public awareness of current events pertinent to homeland security and NJOHSP's overall mission. As a result, NJOHSP messaging that touched on everything from new programming to disinformation, made its way to every platform of nearly every major media outlet in New Jersey.

The Communications team also continued the creation and distribution of its prominent weekly NJOHSP Bulletin, which boasted as many as 6,560 subscribers.

The group has also been the artistic force behind NJOHSP's marketing and events materials, including booklets, brochures, flyers, trifolds, snapshots, intelligence briefs, and posters, all of which are used across every division to educate viewers on NJOHSP's many events, programs, initiatives, and successes.



**NEW JERSEY OFFICE OF  
HOMELAND SECURITY  
AND PREPAREDNESS**

**CONTACT US**

**[communications@njohsp.gov](mailto:communications@njohsp.gov)**

**[njohsp.gov](http://njohsp.gov)**