

Delaware – DSHS

# **State Homeland Security Strategy – Countering and Preparing for Current and Evolving Terrorism Threats**

**Delaware Homeland Security Strategy - Revised**

**Delaware Safety and Homeland Security**

**2015**



## **A Message to Delaware Citizens:**

As Secretary of the Delaware Department of Safety and Homeland Security I am pleased to present the 2015 – 2017 Delaware Homeland Security Strategy.

In Delaware, our homeland security starts at the local level as hometown security. Protecting our nation and state begins with securing every town and each community. Security includes providing our first responders and citizens with the tools and resources necessary to prepare for both the expected and the unexpected. This is a comprehensive strategy that applies to not only the threat of terrorism but also to natural disasters and other man made emergencies that might impact our state. This strategy maintains the all-hazards approach of preventing, responding to, recovering from and mitigating the effects of terrorist acts or other events or disasters. It is the foundation for building plans, organizations and collaboration for our many partners and stakeholders within both the public and private sectors. Solid partnerships enable the state to properly align critical and scarce resources to fulfill our mission of security and safety. This new strategy will guide the development of a homeland security plan that will ensure the people and property of the State of Delaware are protected to the greatest extent possible.

I am confident that you, as a valued partner in this effort will find the 2015 – 2017 Delaware Homeland Security Strategy to be clear and effective guidance. As homeland security threats continue to evolve, it is critical that we as a community continuously review and revise our strategy to meet these changes. The state will remain vigilant in our efforts to address threats before they impact our communities and will strive to mitigate the effects should they ever occur.

I sincerely would like to thank the numerous members of Delaware's public safety community who dedicate their lives and time keeping our state and citizenry safe. Working in concert and proactively will help us remain prepared to handle current and shifting threats to our state and our nation.

Lewis D. Schiliro

Secretary, Department of Safety and Homeland Security



## Introduction

Throughout the past few years, Delaware has made significant progress in its preparation to deal with terrorism. By developing capabilities and expanding its capacity to identify, disrupt and respond to terrorism the state is better placed today to protect its citizens and property than at any time before.

The challenge we face is dealing with the constantly evolving nature of terrorism. It requires continual evaluation and realignment of our priorities, strategy and tactics to the changing threat picture. To that end, Delaware must maintain a visionary approach to combating terrorism while never failing to ensure that our fundamental counterterrorism capabilities are alert, strong and receiving the resources necessary to protect us.

Leveraging the insight and expertise from a cross section of the state's security and safety professionals, the executive leadership of the Delaware Department of Safety and Homeland Security has developed this Terrorism Preparedness Strategy as set forth here. This document will offer direction and guide a unity of effort on the part of every agency and individual entrusted with the safety of our citizens and their property. In order to anticipate ever changing threats it is vital that we not allow preconceived notions or bias to affect our judgment and that we continually think "outside of the box" while remaining fully informed on terrorism developments domestically and internationally. We live in a threat environment unlike anything seen before. It is an age where would-be terrorists can be recruited, trained and guided from the virtual world of the internet. Countering this is a daunting task.

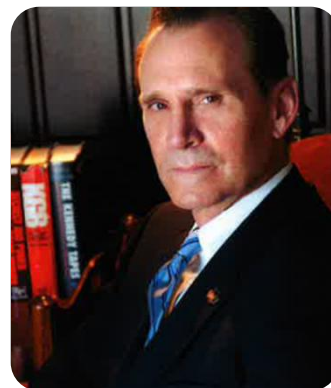
Delaware recognizes that at the same time disaster occurrences are escalating, the resources available to support prevention and response activities are rapidly diminishing. New initiatives will promote greater community commitment, unity of effort and purpose, with the goal of achieving more effective and efficient emergency preparedness and management outcomes for the state. Utilizing available resources from partners in the public and private sectors to sustain or enhance threat assessment, identify and mitigate vulnerabilities and more systematically address non-conventional threats such as biological, chemical or radiological terrorism, or cyberattacks is essential to assuring robust and resilient capabilities to counter the changing threat picture.

The information and guidance provided by the Department of Safety and Homeland Security staff, as well as numerous advisors outside the Department, were instrumental to the successful completion of the Strategic document and shall continue to be critical to implementing the proposed framework.

This agency greatly appreciates all who continue to contribute in this important preparedness initiative.

Thank you – Remain Prepared,

Raymond Holcomb  
Delaware Homeland Security Advisor



## Handling

This strategy is designed to inform citizens, emergency responders, and private sector partners for Delaware's Homeland Security Strategic mission, goals and objectives. Certain information contained here within is derived from sensitive sources pursuant to 29 Del. C. 100 Sensitive Source Documents, research and other related materials which are exempted from Freedom of Information Act (FOIA) statutes and restricted from public use.

Any comments, suggestions, or questions related to this document should be directed to the Department of Safety and Homeland Security, State Homeland Security Advisors office at:

303 Transportation Circle  
PO Box 818  
Dover, DE 19903

## Table of Contents

<b>Overview .....</b>	<b>6</b>
<b>Delaware in Perspective and vulnerabilities .....</b>	<b>7</b>
<b>Developing the Strategy.....</b>	<b>8</b>
<b>Considering Strategic Needs.....</b>	<b>9</b>
<b>Engaging Evolving Threats.....</b>	<b>10</b>
Active Shooter.....	10
Improvised Explosive Devices.....	11
Mass Transit Targeting.....	11
Soft Infrastructure Targeting.....	12
Cyber Attack.....	13
Biological and Agricultural Terrorism.....	13
Government Specific Targeting.....	14
Emerging Threats.....	14
<b>Risk Management for Delaware Threats.....</b>	<b>16</b>
<b>Appendix A – Missions, Goals and Strategies.....</b>	<b>18</b>
<b>Appendix B – Delaware Terrorism Threat Graphic.....</b>	<b>19</b>
<b>Appendix C – Homeland Security Advisory Council.....</b>	<b>22</b>
<b>Appendix D – Terrorism Plots, Tactics and Techniques.....</b>	<b>24</b>
<b>Appendix E – Acronyms, Concepts and Definitions.....</b>	<b>25</b>
<b>Documents and Publications Referenced.....</b>	<b>27</b>

## Overview

Over the course of several years, a great deal of time, effort and resources have been invested across the state to increase terrorism preparedness efforts. Delaware's purpose in creating a Terrorism Preparedness Strategy is to ensure the state is ready to perform its life safety mission against the complete array of possible threats and that our preparedness goals are achieved in a manner that is effective, efficient and sustainable. This Strategy will serve as a useful tool for state leaders to identify and prioritize capability goals and ensure corresponding needs are met through future initiatives.

The 2014 Quadrennial Homeland Security Review, released June 18, 2014, identified the nation's homeland security strategic missions as:

- Preventing terrorism and enhancing security
- Strengthening national preparedness and resilience
- Safeguarding and securing the cyber space domain
- Securing and managing borders
- Enforcing and administering immigration laws

Delaware will implement these national imperatives at the state and local levels. It will require a unity of effort among security and response partners as well as end users and stakeholders. To that end the state will pursue the following goals in alignment with National Security Strategic Missions;

- Preventing terrorist attacks within the state
- Countering violent extremism and recruitment within the state
- Enhancing and reinforcement of state preparedness
- Mitigating threats and hazards
- Identifying and mitigating vulnerabilities
- Providing effective emergency response
- Promoting rapid and enduring recovery
- Strengthening the security of critical infrastructure
- Securing data and information enterprises
- Furthering law enforcement, incident response and reporting capabilities
- Strengthening the cyber ecosystem
- Intercepting hazardous and/or radiological materials which could be weaponized
- Identifying and defending ports of entry by hostile entities
- Identifying and verifying population status
- Ensuring citizens' legal status and deterring discriminatory actions
- Disrupting and dismantling terrorist and criminal actors who exploit immigration law

*These Missions, Goals and Objectives have been combined in a formatted display which can be referred to in Appendix A for details.*

*The State's Vision and Mission statements are simple, concise and germane. They are the bedrock from which the entire strategy will be built.*

**Vision:** The pre-eminent example for security, safety and preparedness.

**Mission Statement:** The Delaware Department of Safety and Homeland Security (DSHS) endeavors to fully support and protect our citizens, our communities, our first responders and our infrastructure. As such, we must work in concert to build, sustain and improve our capabilities to prevent against, respond to, mitigate and recover from terrorism threats and other hazards ensuring a more resilient state.

### Delaware in Perspective and Vulnerabilities

Delaware is home to approximately 898,000 people ranking it as the 45th most populous state. Although Delaware is the second smallest state in the country, it remains one of the most densely populated. The state occupies part of the peninsula between the Delaware and Chesapeake Bays, making it heavily reliant on key causeway connections for commerce and travel. Delaware is divided into three counties: New Castle, Kent, and Sussex. Historically, industrialized New Castle County has contrasted with the other two counties, which have been chiefly agrarian in nature. Currently, 60 percent of the population resides in New Castle County in and around the city of Wilmington, the state's only metropolitan area. Dover, located in Kent County in the center of the state, is Delaware's capital. There are 1,400 sites which use or store hazardous materials for various commercial and industrial interests. The waterways of our local area witnesses at least 3.6 million tons of petroleum products in transit to and from global markets. There are approximately 1800 miles of petroleum and related logistical pipeline within the state. The state has 100,000 tons of hazardous materials transported on over 3,500 miles of roadways. There have been instances of radioactive materials being transported by water, air and road in our state. The state is home to numerous critical services in fact, the finance, insurance and real estate industry contribute more to the state's economy than any other industry. More than three-fifths of companies listed on the New York Stock Exchange have incorporated in the state due to the chancery courts. Delaware is situated among major transportation corridors such as Interstate 95, railway systems both passenger and logistical, a ferry system that connects state partners, a canal system, a major strategic military base, a major water port, a commercial airport and numerous other sites and resources. Delaware's agricultural industry is vital to sustaining a strong economy as well. The poultry industry is the mainstay of the state's agricultural revenue generation. Sussex County particularly is nationally recognized as the center of broilers production. Delaware is a small but complex state with numerous interests, industries, cultures and concerns.

As with many states across the nation Delaware may experience a host of hazards or threats at any moment. These hazards include but are not limited to;

- Natural hazards such as: flooding, dam and levee failures, drought, earthquakes, winter storms, hurricanes and tropical storms, temperature extremes, severe convective storms, sinkholes, tornadoes and wildfire.
- Technological hazards such as: cyber-attacks, hazardous materials incidents, radiological accidents and transportation-based hazardous materials incidents.

- Infrastructure failures such as: communications failure, petroleum shortages, pipeline accidents, power outage/failure, structural failures and transportation system failures.
- Public health emergencies such as: animal and plant disease, human health or pandemic emergencies and mass casualty incidents.
- Social and civil disturbances are events that are resultant from a breakdown in civil control, war, and other wide scale emergencies or actions. These may include: an enemy attack, mass migration or repatriation events, public disorder or civil unrest, school emergencies large, structure fires.

Current global trends have highlighted the increasing, ever changing concerns of terrorism. Terrorism related hazards are violent or criminal acts dangerous to human life and property and which violate federal or state law. Such acts are intended to intimidate or coerce a civilian population, influence government policy or affect the conduct of a government. In addition to conventional threats, such as active shooter attacks and improvised explosive device attacks against crowded venues, terrorism threats include agricultural and biological terrorism, chemical and radiological terrorism, and internet attacks against commercial, government and utility systems that have direct influence on our critical infrastructure.

Delaware remains a unique state with contrasting and complimentary industry, economy, populations, geography and interests which may present themselves as lucrative targets for terrorists. The state requires a strategy which can be realistically implemented, is easy to incorporate and flexible enough to meet developing threats and hazards in an ever changing world. This open strategy will help guide state, county and local municipal partners to ensure the security and safety of all residents, guests, industry and businesses throughout Delaware.

### Developing the Strategy

Delaware has maintained a robust and resilient terrorism preparedness doctrine since September 11, 2001 and will continue to do so in the future. The state will adapt to future environments and threats as they evolve. Delaware will continue to adamantly assist first responders with the support and resources they need. Delaware recognizes that at the same time disaster occurrences are escalating, the resources available to support response activities are rapidly diminishing. Current forecasts demonstrate this trend is unlikely to change any time soon and will challenge Delaware's ability to maintain and deliver terrorism preparedness mission capabilities.

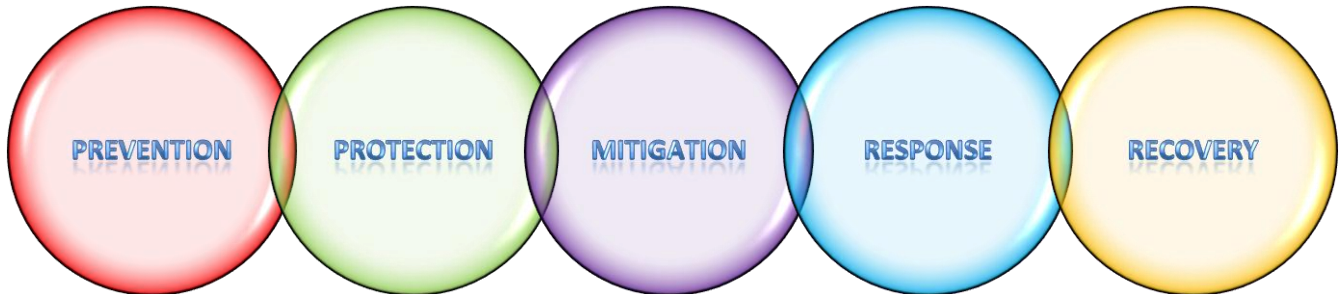
Delaware's 2015 -- 2017 initiatives will provide a more flexible and adaptive structure capable of responding to new situations, capitalizing on opportunities, and quickly adjusting to shifting environments. New initiatives will promote greater community commitment, unity of effort and purpose among all members of the emergency management team, with the goal of achieving more effective and efficient emergency management outcomes for the state. The 2015 – 2017 initiatives are:

- Nurturing a statewide "Whole Community or Unity of Effort Approach" for emergency management
- Becoming as efficient and effective as possible with existing resource levels



- Building the state's capacity to stabilize and recover from a catastrophic event
- Enhancing the state's ability to learn and innovate from past, present and future experiences

In order to meet these initiatives, Delaware will base strategy on the five national mission areas while shifting from the all hazards approach used in previous years to a more terrorism centered approach.



### Considering Strategic Needs

In order to address ever evolving terrorism threats it is necessary to understand the variables that impact strategy development. These variables include, but are not limited to:

- Evolving terrorist threats
- Government budget constraints
- Aging critical infrastructure
- Technical innovation and dependency
- Increased reliance on vulnerable information systems
- Regional interdependencies
- Climate change
- State demographic shifts

Delaware will carefully consider these variables while developing strategy which will impact decision making, objectives priorities and plans.



## Engaging Evolving Threats

Ever evolving terrorist threats will continue to demand consideration and resources to ensure the citizenry of the state remain safe. The people of Delaware must remain confident in their belief that their government provides security and resiliency. Although the death of Al-Qaeda leader Osama bin Laden proved an important victory in the war on terrorism, it still remains far from over. We must all remain mindful and vigilant on a state and regional level. We should understand that since 9/11, at least sixty (60) publicly known attempted terrorist operations against the nation have been thwarted, of which fifty one (51) can be categorized as homegrown violent extremist (HVE) plots (see Appendix D). It is evident that homegrown terrorism has become more attractive to terrorist networks as it reduces the need for command and control and funding while reducing the risk of detection.

Delaware has identified eight (8) areas of concern that must be addressed with tailored strategies that are designed to ensure that the public, our infrastructure, and our government are protected from terrorist attack. These areas of concern include but are not limited to: Active Shooters, Improvised Explosive Devices, Mass Transit Targeting, Soft Infrastructure Targeting, Cyber Attack, Biological and Agro-terrorism, the Targeting of Government Officials, and Emerging Threats. Further definition and discussion of each threat concept is provided hereafter.



**The Active Shooter threat:** An Active Shooter is any individual (or group of individuals) who participates in a random or systematic shooting spree, with the intent to continuously harm others. An active shooter's overriding objective is mass murder, rather than criminal conduct such as robbery, kidnapping, or the destruction of property. The same intent to achieve mass murder may be accomplished using edged weapons and explosives. Recent history has shown that these attacks can be near spontaneous or highly calculated. This threat is magnified by the fact that in most cases the attacker(s) is resigned to die in the effort. The calculated or planned attack offers increased opportunity for disruption by an alert community aware of pre-operational indicators. In regard to spontaneous attacks individuals who are so inclined usually present more nuanced pre-attack indicators. Persons who are trained in identifying these indicators and who have some familiarity with the individual of concern can play a role in preventing such an attack.

With the exception of terrorists who have received at least some para-military training and intend to fight on with the goal of achieving maximum media coverage and psychological impact, most active shooter attacks end within minutes. Unless armed security is in a position to respond instantly, those in danger will have to make immediate decisions regarding their own personal safety. A robust awareness and training campaign for the general population, and particularly those who work at or near high risk venues, can be instrumental in disrupting and mitigating the effects of such an attack. The public must be empowered to take a role in its own protection through training programs that emphasize pre-attack indicators and that teach survival techniques such as "Run-Hide-Fight."

Our law enforcement officers must receive regular training in the most currently accepted tactics for responding to active shooter incidents. Lives will be saved through training and clarity of purpose.



**Improvised Explosives Devices (IEDs):** Traditionally employed by insurgent groups and terrorist organizations, the use and sophistication of IEDs continues to increase including several attacks, multiple disruptions, and countless hoaxes across the United States. IEDs consist of a variety of components that include a power source, a switch, an initiator, a main charge, and a container. IEDs may also include additional materials such as nails, glass, or metal fragments designed to increase the amount of shrapnel propelled by the explosion. An IED can be initiated by a variety of methods depending on the intended target.

Many commonly available materials, such as fertilizer, gunpowder, and hydrogen peroxide, can be used in constructing IEDs.

Examples of IED targeting in the United States include iconic mass gathering events like the 2013 Boston Marathon bombing and the 1996 Centennial Olympic Park bombing in Atlanta. There have been a number of localized events including a disrupted IED attack during a 2011 Martin Luther King Jr. march in Spokane, WA. Less lethal but more frequent, isolated targeting of businesses or individuals has occurred; and an increase in hoax devices and verbal or written threats have become a recurring disruption to schools and businesses. In order to counter the growing threat of IED's we must focus on citizen and first responder awareness of pre-attack indicators; including identifying individuals with an unjustified interest in explosives or efforts to acquire quantities of bomb making materials. Public awareness is the first defense in preventing IED attacks. First responders must receive regular training incorporating the most current developments in IED construction and use, and first responders must be equipped with the proper equipment for identifying and safely disrupting IEDs.



**Mass Transit Targeting:** Mass Transit systems face a variety of threats and hazards from terrorist attacks, cyber-attacks, natural disasters, aging and failing infrastructure, and accidents. Specific domestic threats against mass transit, as well as a number of successful international attacks, illustrate the risk to these systems. Additionally, due to interdependencies, cyber-attacks against infrastructure can also impact mass transit. As an example, passenger and freight rail facilities often depend on electric power, communications, and information technology to perform core operations. Marine

transportation, including ferries, cruise ships and recreational boats, faces the same risk due to cyber reliance, port vulnerability, and shore-side intermodal connections. Public awareness of pre-attack indicators is the best counter to attacks against mass transit systems. As mass transit offers unique security and rescue challenges first responders must have the training and equipment necessary for an effective response to an attack of any kind on mass transit facilities.

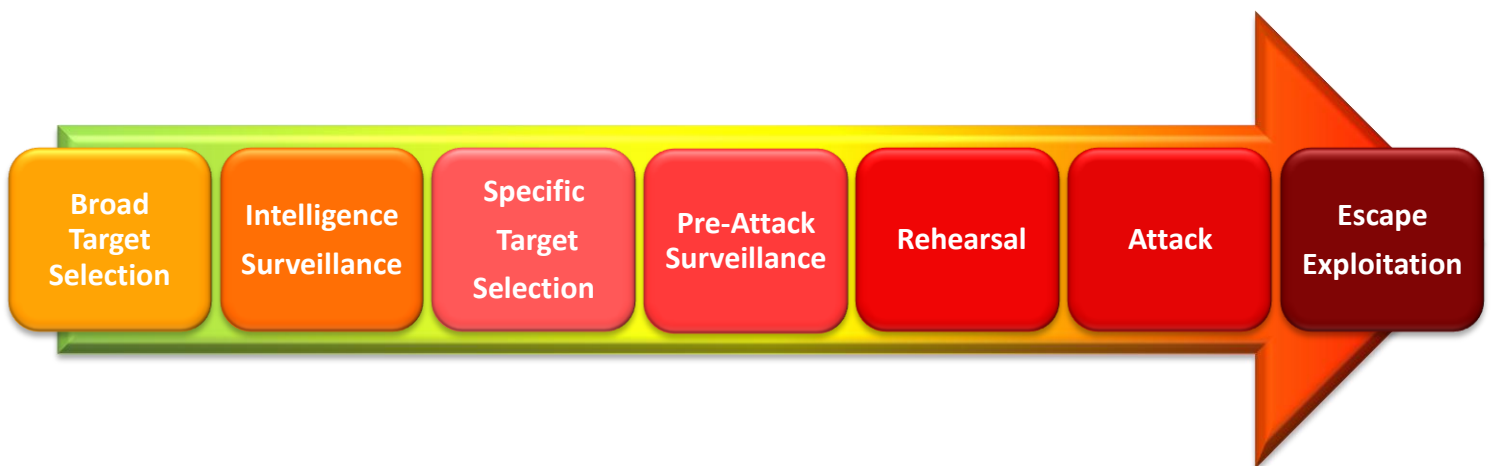


**Soft Infrastructure** or lightly protected Critical Infrastructure and Key Resources (CIKR) offer terrorists target opportunities with potential for high psychological and physical impact. CIKR constitutes any system, asset and network, physical or virtual, which are so vital to the state and to the U.S. that their incapacitation or destruction would have a debilitating effect on personal security, state and national economic security, public health or safety, or any combination thereof. Key resources are publicly or privately controlled resources essential to the minimal operations of the state economy and government. Power production, storage and transmission facilities; communications

transmission facilities; central collection points of commerce, such as harbors, rail yards, airports, bus terminals; petro-chemical processing and transmission facilities, are examples of CIKR that when lightly protected qualify as “soft infrastructure.” The State of Delaware hosts many such resources and facilities. Efforts must be made to “harden” vulnerable points wherever they exist and to regularly monitor and review security arrangements. This will require close cooperation between government and the public and private sectors. Educating all sectors on pre-attack indicators and the need to report any suspicious activities are critical to protecting our infrastructure and resources.

Individuals planning a terrorist attack follow a discernible cycle and that cycle and behaviors associated with it can be detected. The terrorist attack cycle begins with development of an initial target list. The cycle progresses to initial and low level surveillance in an attempt to identify security postures and vulnerabilities.

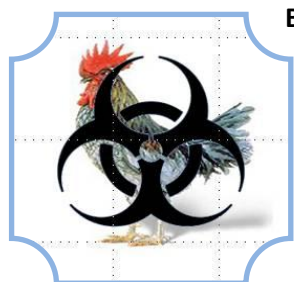
Educating the populace on key elements of the planning cycle creates a security force multiplier that is critical to identifying and disrupting terrorist attack efforts. A vigilant populace, sensitized to pre-attack indicators is the first line of defense. Our safety is the responsibility of both public officials and private citizens.





**Cyber-attack** is becoming an ever increasing national, regional and state concern. Recent events demonstrate the threat is evolving and real. Numerous vulnerabilities in government, commercial, educational, public and private sectors highlighted in the press almost every day prove the case that the most far reaching and intrusive threat we face for the foreseeable future concerns the internet and the avenues for attack it offers terrorists, state-sponsored individuals and rogue criminal hackers. Our vast reliance on cyber technology has created an equally vast vulnerability. As terrorists continue to turn to unconventional and asymmetrical weapons, cyber warfare threats continue to increase. Additionally, more and more tech-savvy terrorists and criminals are coming of age and recognize the value of cyber systems to inspire and recruit would-be terrorists as well as virtually training and directing their attacks.

Because most critical infrastructure is networked and operated through computers, the potential threat from cyber-terrorism has become alarming. Almost routinely, hackers have demonstrated the ability to gain access to sensitive information and disrupt the operation of crucial services. Growing dependence on information technology and a societal appetite for social media has created a new form of vulnerability, giving terrorists the chance to identify targets that previously were unassailable, such as the identities of U.S. military personnel and their families. It now appears that the more technologically developed a country is; the more vulnerable it is to cyber-attack. Delaware is no exception to this threat. The state should develop threat awareness programs which share critical, time of the essence information with all sectors to ensure an effective effort to detect, disrupt and recover from all cyber threats. Cyber-attacks are not limited by geographical boundaries. Like a deadly pathogen, they can spread from system to system and gain access to the most crucial information or control systems. There is no indication that this threat will abate in the foreseeable future. Delaware must have a “whole community” approach in dealing with this challenge. It will require resources, constant vigilance, proactive tactics and strategic vision in order to be successful.



**Biological and Agricultural Terrorism** continue to be threats that must not be ignored. While incidences where criminals and terrorists have utilized pathogens to attack agricultural targets are sparse, it can be logically argued that the only difference between naturally-occurring infectious diseases and biological warfare agents is “intent”. The same mechanisms that monitor and provide intelligence for agricultural and biological scenarios which occur in nature, can function just as well regardless of how the agent is administrated.

That said, terrorists can strike without notice and they can pick the time and place of their choosing. In the absence of a credible claim of responsibility, valuable time may pass before it becomes clear that the outbreak is an intentional or criminal act. The ability and will to “weaponize” a naturally occurring disease must never be dismissed. If a disease can be found in nature we must assume it can be manipulated for criminal intent and we must be ever vigilant for the suspicious acts and warning signs. Any weapon that can be improvised using available and accessible materials is a terrorist weapon of first choice. Similarly, any weapon that stands a reasonable chance of inflicting catastrophic economic and mass psychological damage is a weapon that we must respect and defend against. Delaware is heavily



reliant on agriculture for a viable economy. The deliberate or natural introduction of a pest or disease could have serious consequences for the state and the region.

Delaware must continue to monitor the health of this pivotal industry by performing sustained observation and surveillance for contagious diseases in all crops and domestic animals. In the event of a significant outbreak the Department of Agriculture will need the assistance of numerous organizations and agencies to effectively contain and eliminate the threat. Emergency response plans must be current and must be exercised. Public awareness programs are a critical piece to this effort. The state should develop public awareness programs which effectively share information among all stakeholders at every level to ensure that they understand the threat and conduct surveillance to detect it at the earliest possible moment.



**Government Specific Targeting** is the intentional selection of law enforcement officers, first responders, military personnel, government executives and associated infrastructure for targeting and terrorist operations. The occurrence of such acts has been increasing with an alarming upturn in ambush style attacks on law enforcement officers. Groups or individuals may use targeted assassinations of government officials in order to impact response and services, to demonstrate governments' inability to protect the public, and to spread public mistrust. Motives may be political or simply based on revenge.

There are approximately fifty-four (54) state and local law enforcement agencies with over 2,130 sworn officers in Delaware. There are fifty-nine (59) recognized municipalities with thousands of officials who ensure government operates and provides vital services to the general population. Delaware also has National Guard, Active Duty and Reserve military personnel, assets and infrastructure located throughout the state. These resources provide numerous targets of opportunity as police, military and other officials, both directly and indirectly, are viewed as instrumentalities of the government. In that sense, law enforcement, military personnel and local government agents and officials have both a tactical and strategic value to terrorists. Local Military and Law Enforcement officers' role in combating terrorism is critical, as they too are victims of such violence as well as the front line protectors of the state and community. Providing the community an effective awareness and reporting program will ensure law enforcement and government officials are safe and effective at serving and protecting their communities. Establishing positive community relations and demonstrating a mutually beneficial partnership between communities and their officials will benefit all law abiding citizens as well as those sworn to serve them and protect them.



**Emerging threats:** Such threats can be difficult to identify and to plan for; however, it can never be assumed that terrorists will not adjust their tactics or their targets. New technology often brings with it new vulnerabilities. These vulnerabilities should be identified and security protocols should be designed and implemented to address them. Terrorist leadership and ideologies change regularly and with those changes often come new directives aimed at "punishing" perceived enemies. It is critical that Delaware maintain close

working relations with federal and regional security agencies in order to keep current on new threats. In this regard the Delaware Intelligence and Analysis Center (DIAC) perform a key role as the primary conduit of threat related information. The DIAC administers numerous security and information functions that serve to protect the people and the property of Delaware. The sharing of local, national and international information is important to anticipating trends in terrorism and designing revised collection efforts and educational programs that can head off emerging dangers. Developments in Unmanned Aerial Vehicle (UAV) technology, computer intrusion techniques, internet recruitment and instruction, are among just a few dangerous developments that not so long ago were given little consideration. While watching the horizon we must accept that terrorists are constantly seeking innovative means to circumvent explosives recognition and detection equipment (EDE), to recruit inside actors capable of circumventing ever improving perimeter and access security, and consistently develop and refine tactics that have, in the past, succeeded. As the author Peter Lance says in the title of his book terrorists have *1000 YEARS FOR REVENGE*. They are patient, observant and resourceful. We must be the same. From a tactical standpoint we must try to see things through their eyes. We must understand that from the standpoint of safety, cultural differences can place us at a disadvantage. We must think “outside of the box,” and never assume that terrorists are somehow less astute than we are. No one can predict with any certainty what terrorists might do next, however, we should never again find ourselves in the position, after the loss of innocent lives, asking why we did not consider a certain deadly tactic. If there is one guiding rule for counterterrorism it is that the next attack may look nothing like those that have preceded it.

*The terrorism threats which this strategy currently addresses have been consolidated into an easy to review graphic which can be referred to in Appendix B for details.*



## Risk Management for Delaware Threats

Risk reduction and mitigation efforts will employ the most effective countermeasures against known threats. Proper risk analysis will implement countermeasures that cover a multitude of vulnerabilities. A suitable risk management strategy will in effect, reduce risks to a level that is as low as reasonably achievable and can be tolerated by executive personnel. To achieve this goal, a strategy must incorporate the identification and implementation of such countermeasures. Risk management and security experts realize that of the variables presented in ARM analysis, vulnerabilities are the primary concern. The use of Designed Basis Threats (DBT) is also highly beneficial to providing physical

mitigation, protection and prevention countermeasures for identifiable threats. Recognizing DBT assures an understanding of the threats and can lead to a detailed description of potential adversaries (the design basis threat) which, in turn, become the basis for appropriately designed physical protection systems. Local, state, and federal governments should assess risks to effectively prioritize limited resources. The current trend for Risk Managers and security professionals is to resolve risk concerns with a comprehensive “All Hazards” approach in an effort to limit the impact of events. It may be impractical for decision makers to address concerns by specific threat, especially with dwindling resources and waning public interest. A Sensible combination of proven strategies would be the most judicious approach and offer the most efficient coverage with increasingly limited resources.



*Delaware will continue to utilize the Threat and Hazards Identification and Risk Assessment (THIRA) as a means to highlight threats and relate them to capabilities. This approach will dictate planning, resource allocation and prioritization of efforts.*

The THIRA is a methodology that provides a comprehensive approach for identifying and assessing risks and associated impact. It expands on existing local and state Hazard Identification and Risk Assessments (HIRAs) and other risk methodologies by broadening the factors considered in the process, incorporating the whole community throughout the entire process and by accounting for important community-specific factors. The THIRA consists of the following steps:

- Identify threats and hazards of concern.
- Give threats and hazards context.
- Establish Capability Targets.
- Apply the THIRA for estimating the resources required to meet capability targets.

THIRA allows Delaware an opportunity to understand threats and hazards and how they may impact the state according to time of occurrence, seasons, locations, and other community related factors. This knowledge allows the state to establish informed and defensible capability targets and commit proper resources to bridge any gap between an identified target and a current capability. It also provides for

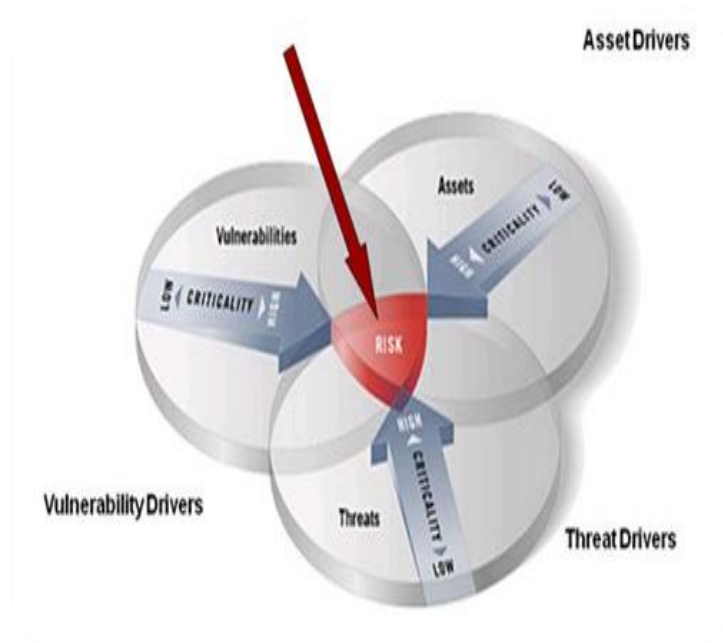


the sustainment to existing capabilities. The capability targets established under the THIRA are assessed through the State Preparedness Report (SPR) which is a self-assessment of preparedness through the lens of 31 Core Capabilities.

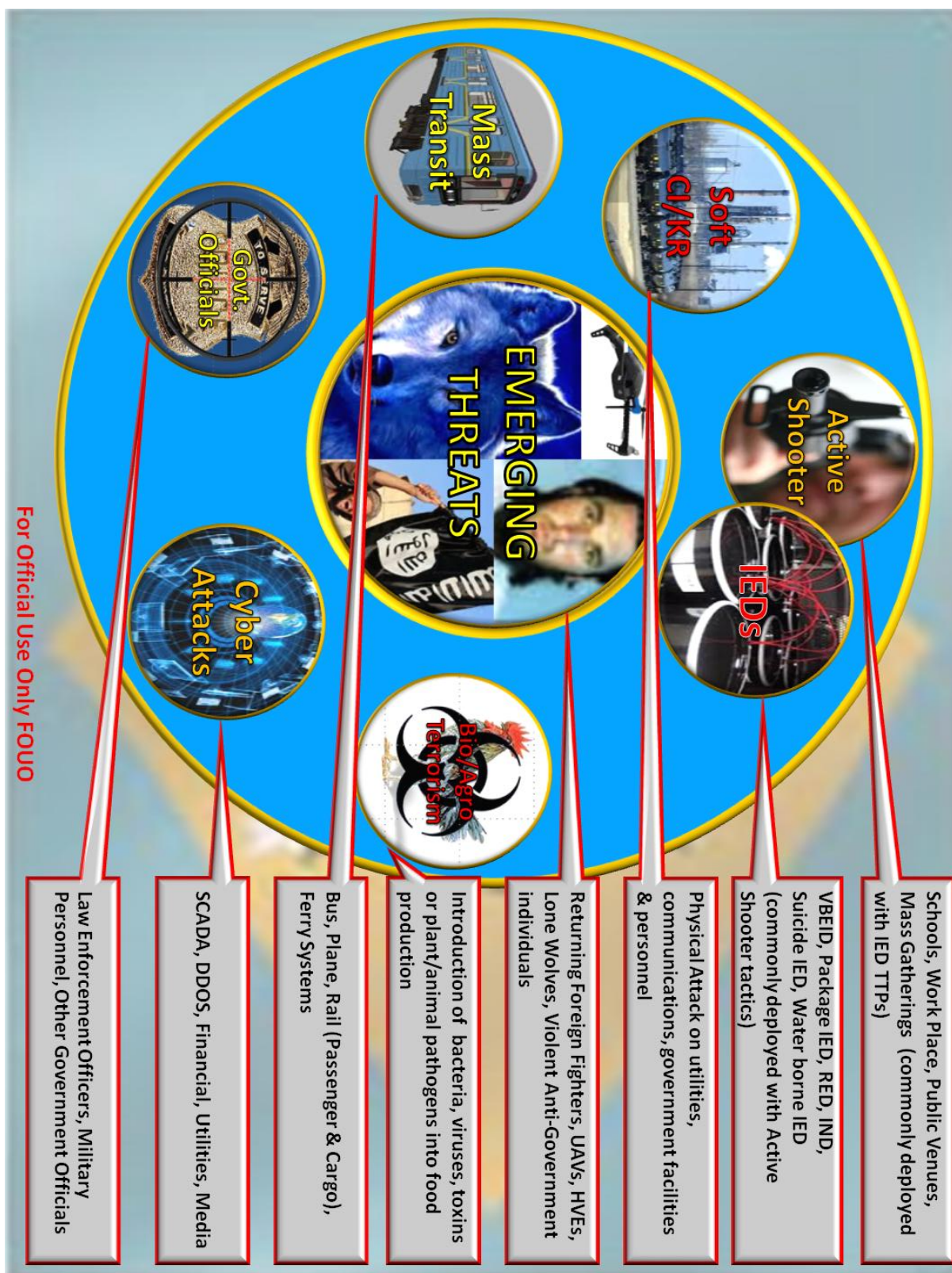
The SPR aggregates the data of the THIRA to achieve a self-assessment of how Delaware is meeting the national goals and priorities. The SPR is gathered along with surrounding states to produce a regional preparedness report by FEMA Region III. The regional reports are then combined to develop the annual National Preparedness Report (NPR) to summarize progress in building sustaining and delivering capabilities outlined in the National Preparedness Goal (NPG).

According to the 2014 NPR, states across the nation need to embrace new approaches to disaster recovery. There will be a major national effort launched for policy and planning initiatives to bring unity of effort to preparedness areas, including critical infrastructure security and resilience, cyber security, recovery capabilities, and even climate change. There will be a concentration for managing the uncertainty of continued resourcing. As budget uncertainties create challenges to preparedness at state and local levels of government, states will be required to utilize increased ingenuity, innovations and whole community engagement.

Delaware will meet these challenges head on by implementing the sixteen (16) strategic goals listed in the overview section and displayed in Appendix A of this strategy. Each goal will have supporting objectives to assist in further defining the programs, initiatives and steps that should be taken to meet the overarching goal. These goals and objectives are envisioned to be applicable for a number of years. Delaware will implement this strategy through coordinated and integrated programs, policies and projects that support the defined goals and objectives. Effective implementation requires agencies, organizations, communities and governments to all work to plan, invest and support each other in this endeavor.



 <b>Delaware - Terrorism Threat Mitigation Framework</b> 	
<b>Mission 1: Preventing terrorism and enhancing security</b>	
<b>Goal 1.1: Preventing terrorist attacks within Delaware</b>	Objective 1.1.1: Analyze, develop and provide terrorism intelligence Objective 1.1.2: Deter, delay, defeat and disrupt terrorism operations Objective 1.1.3: Strengthen transportation security
<b>Goal 1.2: Countering violent extremism and recruitment within the state</b>	Objective 1.2.1: Identify and counter recruitment operations Objective 1.2.2: Provide awareness information for suspicious activity reporting
<b>Mission 2: Strengthening state preparedness and resilience</b>	
<b>Goal 2.1: Enhance and reinforce state preparedness</b>	Objective 2.1.1: Empower individuals and communities to strengthen and sustain preparedness Objective 2.1.2: Build and sustain core capabilities to prevent, protect, mitigate, respond and recover from all threats
<b>Goal 2.2: Mitigate threats and hazards</b>	Objective 2.2.1: Assist federal, regional, state and local partners in establishing community programs Objective 2.2.2: Establish, exercise and enforce plans, policies and standards
<b>Goal 2.3: Identify and mitigate vulnerabilities</b>	Objective 2.3.1: Provide and utilize Risk Analysis tools for capability gaps and vulnerability identification Objective 2.3.2: Enhance intelligence collection, analysis and dissemination to stakeholders for consideration and action
<b>Goal 2.4: Provide effective emergency response</b>	Objective 2.4.1: Conduct standardized and unified incident response operations Objective 2.4.2: Provide timely and appropriate disaster assistance Objective 2.4.3: Enable and enhance emergency response communications
<b>Goal 2.5: Promote rapid and enduring recovery</b>	Objective 2.5.1: Facilitate continuity and restoration of essential service and functions Objective 2.5.2: Support local governments and communities to rebuild and integrate smart mitigation processes
<b>Mission 3: Safeguarding and securing the cyberspace domain</b>	
<b>Goal 3.1: Strengthen the security of critical infrastructure</b>	Objective 3.1.1: Enhance the exchange of information and intelligence on critical infrastructure threats Objective 3.1.2: Provide real time situational awareness capabilities to users and administrators Objective 3.1.3: Identify and realize interdependencies and cascading affects of infrastructure failures Objective 3.1.4: Develop policies, plan and procedures to enhance cyber security
<b>Goal 3.2: Secure state government data and information enterprises</b>	Objective 3.2.1: Acquire cyber technology that fortified, compatible and cost effective Objective 3.2.2: Equip networks with innovative tools, protocols and hardware Objective 3.2.3: Ensure policies and protocols are practiced consistently
<b>Goal 3.3: Further law enforcement, incident response and reporting capabilities</b>	Objective 3.3.1: Respond and assist in recovery of cyber incidents Objective 3.3.2: Deny, deter, defend, disrupt and investigate cybercrime
<b>Goal 3.4: Strengthen the Cyber Ecosystem</b>	Objective 3.4.1: Develop highly skilled cyber security agencies and personnel Objective 3.4.2: Enhance public awareness and promote individual security measures Objective 3.4.3: Advance capacity, standards and cooperation
<b>Mission 4: Securing and managing borders</b>	
<b>Goal 4.1: Intercepting hazardous or radiological materials to be used as weapons</b>	Objective 4.1.1: Anticipate CBRNE threats Objective 4.1.2: Identify and interdict illegal acquisition and transport of CBRNE materials
<b>Goal 4.2: Identify and defend ports of entry for hostile entities</b>	Objective 4.2.1: Detect, locate, and prevent entry of hostile actors at ports of entry Objective 4.2.2: Prevent illegal imports and exports
<b>Mission 5: Enforcing and administering immigration laws</b>	
<b>Goal 5.1: Identify and verify status known populations</b>	Objective 5.1.1: Promote lawful immigration Objective 5.1.2: Effectively and fairly administer immigration services
<b>Goal 5.2: Ensure legal status of citizens and deter discriminatory actions</b>	Objective 5.2.1: Promote lawful integration of immigrant populations Objective 5.2.2: Provide supportive environment for legal residents
<b>Goal 5.3: Disrupt and dismantle terrorist and criminal actors exploiting immigration law</b>	Objective 5.3.1: Arrest, detain, and remove high risk individuals Objective 5.3.2: Detect and defeat threats to public safety and security





# Outreach by Threat Area

## ACTIVE SHOOTER

- ALERT—SOP for responding to active shooters
- Christiana Mall, NCC Airport, Lewes Ferry TTX
- School Safety Program, mandatory protocols for active shooter training twice per year



## IMPROVISED EXPLOSIVES

- Education
- Realistic exercises that reflect Delaware specifics
- Reach the appropriate audience
- Currently reviewing outreach procedures



## MASS TRANSIT

- DIAC CIKR Planner—focus on greatest vulnerability
- How do we protect hundreds of miles of rail line?
- Power grid attacks that impact substations—is there presently a minimum amount of protection? Vandals vs. saboteurs



## CYBER ATTACK

- Department of Technology & Information has an extensive system in place to prevent attacks on the State network.
- DTI Regularly performs penetration tests to identify areas of concern



## BIOLOGICAL/AGROTERRORISM

- US Food and Drug Administration created the Strategic Partnership Program Agroterrorism (SPPA)
- Initiative, a joint effort of the FBI, DHS, USDA and FDA to Help Secure the Nation's Food Supply



## GOVERNMENT OFFICIALS TARGETING

- Evaluate & adjust for specific threats to LEO & Govt Officials
- Enhance community relations programs to assist in threat identification



## EMERGING THREATS & CONCERNS

- Outreach to the community to educate about:
  - Returning Foreign Fighters
  - Homegrown Violent Extremists
  - Violent Government Subversives
- Provide a means for suspicious activity reporting
- UAV legislation & Regulation



For Official Use Only FOUO

## Threat Description Table

Act or Target	Threat Actor/ Cause	Probability	Mitigation Efforts	Impact for Delaware	Interaction with DE Events/Locations
Active Shooter Ex: Navy Yard Shooting Paramus Mall Shooting	<ul style="list-style-type: none"> <li>Lone Actor</li> <li>International or Domestic Terrorists</li> </ul>	<b>Based on Analysis</b>	<ul style="list-style-type: none"> <li>Outreach</li> <li>SAR Reporting</li> <li>Training/Exercises</li> <li>Response SOPs</li> </ul>	<ul style="list-style-type: none"> <li>Casualties</li> <li>Psychological</li> <li>Political</li> </ul>	<ul style="list-style-type: none"> <li>•Christiana Mall</li> <li>•Dover Mall</li> <li>•UD Events</li> <li>•Dover Downs Events</li> <li>•Statewide Festivals</li> </ul>
Complex Attack (IED) Ex: Boston Marathon Attack 2010 Attempted IED in Times Square	<ul style="list-style-type: none"> <li>Lone Actor</li> <li>International or Domestic Terrorists</li> </ul>	<b>Based on Analysis</b>	<ul style="list-style-type: none"> <li>Info Sharing</li> <li>Outreach</li> <li>SAR Reporting</li> <li>Training/Exercises</li> <li>Response SOPs</li> </ul>	<ul style="list-style-type: none"> <li>Mass Casualties</li> <li>Economic</li> <li>Psychological</li> <li>Political</li> </ul>	<ul style="list-style-type: none"> <li>•Christiana Mall</li> <li>•Dover Mall</li> <li>•UD Events</li> <li>•Dover Downs Events</li> <li>•Statewide Festivals</li> </ul>
CIKR Targets: •Mass Transit Ex: 2009 Attempted IED in NYC subways •Soft Infrastructure Ex: Silicon Valley Substation	<ul style="list-style-type: none"> <li>Lone Actor</li> <li>International or Domestic Terrorists</li> </ul>	<b>Based on Analysis</b>	<ul style="list-style-type: none"> <li>Info Sharing</li> <li>Protective Measures</li> <li>Training/Exercises</li> </ul>	<ul style="list-style-type: none"> <li>Casualties</li> <li>Economic</li> <li>Psychological</li> <li>Political</li> </ul>	<ul style="list-style-type: none"> <li>•Amtrak</li> <li>•DART</li> <li>•Nearly 24,000 non-farm private establishments in DE</li> </ul>
Cyber Attack Ex: 2014 E-Bay Attack 2014 Montana Health Department	<ul style="list-style-type: none"> <li>Nation-State</li> <li>Transnational Organized Crime</li> <li>Terrorists</li> <li>'Hacktivists'</li> </ul>	<b>Based on Analysis</b>	<ul style="list-style-type: none"> <li>Info Sharing</li> <li>Protective Measures</li> <li>Training/Exercises</li> <li>Mitigation</li> </ul>	<ul style="list-style-type: none"> <li>Economic</li> <li>Psychological</li> </ul>	<ul style="list-style-type: none"> <li>•Banking industry</li> <li>•Chemical industry</li> <li>•Manufacturing</li> <li>•State of Delaware</li> <li>•Large employers</li> </ul>
Bio/Agro-Terrorism/Pandemic Ex: 2002 Al Qaeda documents found 1994 Salad Bars in OR	<ul style="list-style-type: none"> <li>Terrorists</li> <li>Travel/Migration</li> </ul>	<b>Based on Analysis</b>	<ul style="list-style-type: none"> <li>Info Sharing</li> <li>Training/Exercises</li> <li>Mitigation Strategy</li> </ul>	<ul style="list-style-type: none"> <li>Casualties</li> <li>Economic</li> <li>Psychological</li> </ul>	<ul style="list-style-type: none"> <li>•2300 Farms in DE</li> <li>•42% of DE land is farms</li> <li>•43 million chickens</li> <li>•18,000 cattle</li> <li>•6,157 equine</li> </ul>
Emerging Threats Ex: ISIS uses drones for surveillance	<ul style="list-style-type: none"> <li>Foreign Fighters</li> <li>UAV/Proliferation</li> <li>HVEs</li> <li>Govt. Dissidents</li> </ul>	<b>Based on Analysis</b>	<ul style="list-style-type: none"> <li>Info Sharing</li> <li>SAR Reporting</li> <li>Legislation</li> </ul>	<ul style="list-style-type: none"> <li>Casualties</li> <li>Psychological</li> <li>Political</li> </ul>	<ul style="list-style-type: none"> <li>•impacts all other areas</li> </ul>
Government Officials Targeting Ex: NYPD Assassination National LEO Threats	<ul style="list-style-type: none"> <li>Lone Actors</li> <li>Terrorists</li> <li>Criminal Orgs</li> <li>Violent Govt.</li> <li>Subversives/Separatists</li> </ul>	<b>Based on Analysis</b>	<ul style="list-style-type: none"> <li>Info Sharing</li> <li>Community Outreach</li> <li>Protective Measures</li> </ul>	<ul style="list-style-type: none"> <li>Casualties</li> <li>Political</li> <li>Psychological</li> </ul>	<ul style="list-style-type: none"> <li>•Response Capabilities</li> <li>•Law Enforcement</li> <li>•Govt. Services</li> </ul>

**For Official Use Only FOUO**


















## Appendix C – Homeland Security Advisory Council



The Homeland Security Advisory Council (HSAC) consists of the following agencies and individuals list below. The HSAC is a multidisciplinary board that advises Delaware’s Secretary of Safety and Homeland Security on matters of homeland security. It is composed of representatives from fourteen (14) agencies. These agencies include; first responders, federal, state and local government officials, non-government agencies, and private sector concerns. This council is responsible for implementing; Presidential Directives, National Strategy, National Preparedness Guidelines and National Policy for homeland security issues.

Position	Agency	Name
Secretary, Department of Safety and Homeland Security who shall serve as Chair	DSHS	Lewis D. Schiliro
Homeland Security Advisor-DSHS - Co-Chair	DSHS	Raymond Holcomb
Adjutant General of the Delaware National Guard or a designee appointed by the Adjutant General	DNG	LTC Angela Showell
Chief Information Officer for the State of Delaware or a designee appointed by the Chief Information Officer	DTI	Elayne Starkey
Secretary of Department of Natural Resources & Environmental Control or a designee appointed by the Secretary	DNREC	Chief Robert Legates
Secretary of Department of Transportation or a designee appointed by the Secretary	DELDOT	Gene Donaldson
Secretary of Department of Education or a designee appointed by the Secretary	DOE	John Sadowski
Secretary of Department of Agriculture or a designee appointed by the Secretary	DDA	Secretary Edward Kee
Commissioner of the Department of Corrections or a designee appointed by the Commissioner	DOC	Warden David Hall
Delaware State Police Superintendent or a designee appointed by the Superintendent	DSP	Lt. Col. Monroe Hudson
Director of Division of Public Health or a designee appointed by the Director	DPH	Dr. Karyl Rattay
Director Delaware Emergency Management Agency or a designee appointed by the Director	DEMA	Director Jamie Turner
Director Division of Motor Vehicles or a designee appointed by the Director	DMV	Director Scott Vien
Executive Secretary of Delaware Volunteer Firefighter Association or a designee appointed by the Executive Secretary	DVFA	Warren Jones
Chair Delaware Police Chiefs Council or a designee appointed by the Chair	DPCC	Chief Paul Bernat
President Delaware League of Local Governments or a designee appointed by the League’s President	DLLG	Mayor Donald Tinari
Emergency Services Coordinator	Dover Motor Sports	Edward Klima

Position	Agency	Name
Chairman, Administrative Justice Program	Wilmington University	Joseph Aviola
DoD, USAF, 436 AW Antiterrorism Advisor	USAF	Walter Billings
CEO, Delaware Healthcare Association, Emergency Services Organizations	DHA	Wayne Smith
President, Delaware Association of County Governments representative on behalf of New Castle County, Kent County, and Sussex County (Local Governments)	DACG	George Sweeney
AMTRAK, Emergency Management and Corporate Security	AMTRAK	Michael McLean
Chief of Police, Delaware River and Bay Authority	DRBA	Col. Richard Arroyo

## Appendix D – Terrorism Plots, Tactics and Techniques

Terrorist Tactics		Occurrence	Ranking	
	Cyber terror, electronic crimes	1	6	
	Conspiracy, material support, Spying and collaboration	10	3	
	Explosives, VBIED, Suicide Vests, Water Borne IED, etc...	32	1	
	Fire, arson and other destructive means	2	5	
	Small arms and other traditional portable weapons/devices	19	2	
	Weapons of Mass Destruction - Chemical, Biological, Radiological, Nuclear	4	4	
Terrorist Targets		Occurrence	Ranking	
	Aviation assets - aircraft, airports, ATC and supporting structure	6	5	
	Bridges, tunnels, landmarks and other like infrastructure/facilities/assets	2	10	
	Civilians, general public and mass gathering areas/events	14	1	
	Chemical, fuel, other materials infrastructure/facilities/assets	3	8	
	Energy industry infrastructure/facilities/assets	2	9	
	Financial industry, banking infrastructure/facilities/assets	2	11	
	Civil governmental infrastructure/Law Enforcement/First Responders/Personnel	13	2	
	Mass transit (land based) - bus, train, ferry etc...	5	6	
	Military infrastructure/facilities/assets/personnel	11	3	
	Other Industrial infrastructure/facilities/assets	3	7	
	Religious infrastructure/facilities/assets/personnel/landmarks	7	4	

Narratives		# of plots	# of Attackers	Targets	Tactics
<b>Summary</b>	From 2001 to 2014 there were approximately 62 terror plots either foiled or carried out against U.S interests and citizens. Fifty three (53) of those plots had personnel apprehended or neutralized in pre-operational stages or execution. Over 160 personnel were directly involved with many more providing intelligence and other support. Of the targets and tactics, the vast majority utilized or planned to utilize an explosive device of some form against a soft civilian target (Law Enforcement and First Responders, mass gathering, event, known high population density area, etc...). Small arms and combined explosives remain a preference for random lone wolf, homegrown violent extremists and well organized terrorist cells.	53	162		



## Appendix E Acronyms, Concepts and Definitions

**Analytical Risk Management (ARM):** a systematic approach to acquiring and analyzing information necessary for protecting assets and allocating resources to mitigate threats. Utilizes the five (5) step risk management process of; Identify critical resources, analyze current security measures, assess threats, examine vulnerabilities, compute and analyze overall risk.

**Countermeasure:** an action, measure, device or program that reduces an identified risk or lowers the consequences of that risk.

**Critical Infrastructure:** National assets, critical systems, other networks and systems that are vital to the operations of the nation; which their loss, destruction, or degradation would be debilitating to the security, economic security, public health, or any combination of such functions. Such functions provides a means or mechanisms for delivery of critical services, enables people, goods, capital, and information to be distributed for its primary intention. It includes defense, manufacturing, energy production, agriculture, transportation, commerce, and other resources.

**Designed Basis Threat (DBT):** A profile of the type, composition, and capabilities of an adversary and threat. A clear description of known threats defines these conditions and is therefore an essential prerequisite for reasonably assured and effective physical protection. Intelligence and other sources of information related to threats provide information for the specification of requirements for the design and for the performance of physical protection systems to help ensure that security objectives are met.

**Improvised Explosive Device (IED):** A weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract. IEDs can be utilized in various configurations and delivery systems, they are usually categorized by means of delivery and may include; Vehicle Borne Improvised Explosive Device (VBIED), suicide vest IED, water craft IED, mail or package IED and radiological improvised dispersal device.

**Internal Capability:** local community capabilities archived though organic resources - internal capability does not include external resources from a higher levels of government or mutual aid from outside agencies

**Mitigation:** those capabilities necessary to reduce loss of life and property by lessening the impact of disasters. Mitigation capabilities include, but are not limited to, community-wide risk reduction projects; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred.

**Mutual Aid:** An agreement between communities to assist one another on request by furnishing personnel, equipment, and/or expertise in a specified manner

**POETE:** Planning, Organization, Equipment, Training and Exercise

- **Planning:** The development of policies, plans, procedures, mutual aid agreements, strategies, & other publications which comply with laws, regulations, & guidance for performing assigned missions/tasks.

- **Organization:** Individuals, teams, overall organizational structures, & leadership at each level of structure which comply with laws, regulations, & guidance for performing assigned missions/tasks. This includes paid & volunteer staffs who meet qualifications & certifications necessary to perform assigned missions/tasks.
- **Equipment:** Equipment, supplies, & systems which comply with standards for performing assigned missions/tasks.
- **Training:** Content & methods of delivery which comply with training standards for performing assigned missions/tasks.
- **Exercises:** drills & actual events which provide opportunities to demonstrate, evaluate, & improve core capabilities to perform assigned missions/tasks to standards necessary to achieve successful outcomes.

**Prevention:** those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. Prevention capabilities include, but are not limited to, information sharing and warning; domestic counterterrorism; and preventing the acquisition or use of weapons of mass destruction (WMD). For purposes of the prevention framework called for in this directive, the term "prevention" refers to preventing imminent threats.

**Protection:** those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. Protection capabilities include, but are not limited to, defense against WMD threats; defense of agriculture and food; critical infrastructure protection; protection of key leadership and events; border security; maritime security; transportation security; immigration security; and cyber-security.

**Recovery:** refers to those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources

**Response:** those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

**Soft Infrastructure/target:** any infrastructure that due to its inherent design and physical security accouterments appears to be relatively unprotected and more vulnerable to terrorists and criminals. Such infrastructure presents less risk and greater opportunity for successful operations compared to hardened infrastructure.

**Solution Areas:** elements that communities invest in to build & sustain core capabilities (POETEs)

**Terrorism:** the use of force or violence against persons or property in violation of international and United States criminal laws for purposes of intimidation, coercion, or ransom.

**Terrorism Nexus:** a connection of actions, strategies, tactics and procedures which are known to be employed by terrorists to execute operations.

## Referenced Documents and Publications

- Delaware Department of Transportation . (2013). A guide for Stakeholders, Transportation Professional, Elected and Appointed Officials. *Annual Report and Transportation Facts* . Dover , DE, 19901, United States of America: Delaware Department of Transportation .
- Delaware Emergency Management Agency. (2015, February ). Delaware Emergency Operation Plan (DEOP). Smyrna , DE, 19977, United States of America: DEMA, Planning.
- Department of Homeland Security . (2014). *The 2014 Quadrennial Homeland Security Review*. Washington, D.C. 20528: Office of Policy.
- Department of Homeland Security. (2014). *Fiscal Years 2014 - 2018 Strategic Plan*. Washington, D.C. 20528: Office of Strategy, Planning, Analysis, and Risk.
- Department of Safety and Homeland Security . (2012, May 01). Delaware Homeland Security Strategy 2012-2014. *DHSS Version 11* . Dover, DE, 19903, United States of America: Delaware Department of Safety and Homeland Security .
- Federal Bureau of Investigation . (2013, September 16). A Study of Active Shooter Incidents in the United States Between 200 and 2013. Washington Navy Yard, Washington, DC, United States of America: U.S. DOJ.
- Federal Emergency Management Agency . (2011, February 28 ). FEMA Strategic Plan Fiscal Years 2011 - 2014 . *FEMA P-806 / February 2011* . 500 C Street SW, Washington, DC , Washington, DC 20472, United States of America : Department of Homeland Security .
- Federal Emergency Management Agency. (2014, September). FEMA Strategic Plan 2014-2018. *National Advisory Council Meeting Presentation* . 500 C Street SW, Washington, DC 20472, United States of America: FEMA Office of Policy and Program Analysis.
- Lance, P. (2003). *1000 Years for Revenge: International Terrorism and The FBI --- The Untold Story*. 10 East 53rd Street, New York, New York, 10022, United States of America: Regan Books, Harper Collins Publications Inc.
- Office of the Director of National Intelligence . (2014, September 17). The National Intelligence Strategy of the United States of America 2014. *The 2014 National Intelligence Strategy* . Washington, DC, Washington, DC 20511, United States of America: Office of the Director of National Intelligence.
- U.S. Department of State. (2014, April). Country Reports On Terrorism 2013. *Annual Country Reports on Terrorism Bureau of Counterterrorism* , pp. 1-318.
- United States Department of State Publications. (April 2014). *Country Reports on Terrorism 2013*. Washington, D.C. 20520: Bureau of Counterterrorism.

W. Craig Fugate, A. F. (2013, April 01). FEMA Administrator's Intent Priorities Fiscal Years (FY) 2015-2019. *Memorandum of FEMA Administrators Intent* . 500 C Street SW, Washington, DC , Washington DC, 20472, United States of America: U.S. Department of Homeland Security.