The National Guard Cyber Strategy

January 2018

NATIONAL GUARD BUREAU
1636 DEFENSE PENTAGON
WASHINGTON DC 20301-1636

JAN 05 2018

Cyber Strategy for all Soldiers and Airmen

The National Guard (NG) Cyber Strategy outlines the cyber preparedness and cyber activities that support our mission triad areas, which include: Fighting America's Wars; Securing the Homeland; and Building Partnerships. This strategy, and our forthcoming Cyber Strategic Plan, will guide and direct the Title 10 NG force, advise The Adjutants General, and inform our various partners outside of the NG.

Our overall goal is to be the Nation's premier military cyber force for Federal missions directed abroad, as well as Federal and non-Federal activities in the homeland. The NG is manned, trained, and equipped to fulfill Service and joint force prioritized requirements and play a vital role in the Nation's Cybersecurity. The NG Cyber Strategy provides a framework for ensuring the National Guard is "Always Ready, Always There."

I respectfully request your full commitment and support in helping us achieve these goals, and engaging with us to modify or supplement them if required.

Joseph L. Lengyel
General, U.S. Air Force
Chief, National Guard Bureau

Table of Contents

Introduction 5

Chief of the National Guard Bureau Vision 6

The Cyber Threat 6

The National Guard in the Cyberspace Landscape 7

Air National Guard Cyber Forces 8

Army National Guard Cyber Forces 9

National Guard Authorities 9

Existing Department of Defense Cyber Policies Affecting the National Guard. 10

Response to Cyber Events. 11

Strategic Goals 12

Strategic Goal 1: Support the warfight by building and fully integrating National Guard cyber units into the operational federal mission. 12

Warfight Mission 12

Strategic Goal 2: Protect the Homeland by providing highly trained cyber forces available to support Mission Partner requirements. 14

Homeland Federal, State, Local, Tribal, and Territorial Missions. 14

Strategic Goal 3: Expand and leverage enduring relationships with the Private Sector, Academia and International partners. 16

Public and Private Sector. 17

International Partnerships. 17

Implementing the Strategy 18

Conclusion 19

Annex A: References and Authorities 20

Annex B: Acronyms 21

Annex C: Definitions 22

Annex D: National Guard Cyber Units 28

Introduction

Since 1636, before the ratification of the constitution of the United States in 1788, the National Guard has been "Always Ready, Always There" to support and defend the homeland against all enemies foreign and domestic. The National Guard stands ready to support the Nation in its dual capacity, as an operational reserve for our Federal warfighting mission and as part of a whole-of-nation response to protect the homeland.

The internet is an integral component of the United States' national security, and offers opportunities for economic prosperity and innovation. Threats within the cyber domain span across all sectors of a technologically dependent society, providing threat actors a vast array of methodologies to leverage negative effects upon military and civilian communities. The National Guard prepares for these threats, ranging from nation state-actors to non-affiliated individual criminal activities, and seeks to improve readiness and resiliency against these elusive 21st century threats.

End State: The National Guard is an integral component in helping the Nation achieve unity of effort in Cybersecurity actions in the homeland, and in any cyberspace operations directed by appropriate local, state and federal authorities while recruiting and retaining qualified cyber professionals.

The National Guard Cyber Strategy focuses on the three-core missions of the National Guard: "Fight America's Wars, Secure the Homeland, and Build Partnerships." It supports national level strategies and directives including the National Security Strategy, the Department of Defense Cyber Strategy, Army Cyber Strategy, Air Force Information Dominance Flight Plan, Presidential Policy Directives 8, 21, and 41, and the interagency processes and guidance that shape cyberspace policy and incident coordination. It also layers with existing and informs future Army National Guard and Air National Guard strategic guidance regarding Title 10 cyber activities. This strategy directs action to the staff assigned under Chief of the National Guard Bureau authority; advises The Adjutants General and the National Guard forces under their state control, and informs mission partners of the National Guard's strategy for operating in cyberspace.

The National Guard Cyber Strategy and the companion National Guard Cyber Strategic Plan, provide a framework for the National Guard to develop and train its force as a dual use cyber capability for federal and non-federal missions. It offers guidance to the 54 States, Territories, and the District of Columbia, on the non-federal use of the National Guard in cyberspace, while creating a basic structure for strengthening our cyber defense and security. The National Guard Cyber Strategic Plan builds upon this strategy, by providing a road map of short and long-term strategic initiatives to provide properly manned, trained, and equipped National Guard cyber forces available for prompt mobilization for federal missions, national emergencies, or as otherwise requested by state and federal authorities to answer the call by being "Always Ready, Always There."

Chief of the National Guard Bureau Vision

The National Guard's cyber forces fulfills a vital role in the Nation's cyberspace security, with our three-core missions serving as the guide for our future cyberspace activities. While supporting the cyber warfight is fundamental to the National Guard, integration in local communities, role in the homeland, and enduring partnerships with cyber mission partners is integral to a whole-of-nation response and Cybersecurity unity of effort.

National Guard's three core missions -- fighting America's wars, securing the homeland, and building enduring partnerships at the local, State, Federal and international levels

- 2018 National Guard Bureau Posture Statement: Building a Force for the Future

The Cyber Threat

The frequency and severity of cyber threats are growing at an alarming rate. The barrier to entry into cyberspace for cybercrime, espionage, and attack is low, incentives high, and vulnerabilities abundant. Vulnerabilities often related to outdated software or misconfigured networks threaten vectors against the confidentiality, integrity, and availability of critical systems throughout the United States. To exploit these vulnerabilities, cyber threat actors employ a variety of methodologies usually shared through free internet forums. Cyber-enabled destructive and disruptive attacks already have the potential to affect the property, rights, and daily lives of Americans and the cyber threat environment will continue to become more complex as the "Internet of Things" adds millions of new internet-connected devices to our networks. Ever increasing numbers of actors with increasing skill and tradecraft are entering cyberspace every day, many with malicious intent complicating the efforts of defenders protecting United States National Security.

The Department of Homeland Security, through the Industrial Control Systems Cyber Emergency Response Team, routinely warns systems administrators at critical infrastructure sites in the United States and abroad about sophisticated cyber threats from malicious actors. Department of Homeland Security identified 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered, "so vital to the United States that their incapacitation or destruction would have a debilitating effect on vitality, national economic security, national public health or safety, or any combination thereof." In the Industrial Control Systems Cyber Emergency Response Team Fiscal Year 2016 Annual Vulnerability Coordination Report, security researchers and vendors reported 2,282 vulnerabilities in software affecting United States critical infrastructure. The majority of the vulnerabilities affected the energy, critical manufacturing, and water and wastewater system sectors. Given the low barrier to entry and plethora of technical vulnerabilities, cyber security personnel must work in a collective manner to increase overall effectiveness.

Admiral Michael S. Rogers, Commander, United States Cyber Command, testified to Congress in May 2017 that the United States Cyber Command assessed that several countries have conducted disruptions or remote intrusions into critical infrastructure systems in the United States. Last year, for example, the Department of Justice announced indictments for cyber disruptions of United States financial institutions. The United States Attorney General reported that 46 United States companies suffered combined losses of tens of millions of dollars because of the attacks. In late 2015 malicious cyber actors employed the malware Trojan, BlackEnergy, a type of malware used to attack energy-sector

systems, to disrupt part of the Ukrainian power grid briefly cutting off electricity to hundreds of thousands of Ukrainians. Actors are threatening our nation's critical systems now, underscoring the immediate need to increase capacity.

As the cyber threat environment continues to evolve the National Guard will adapt to keep pace, remaining always ready to help defend the nation in its federal role and to assist at state and local levels at the governor's direction. By leveraging the National Guard's unique authorities as a dual-use capability for both federal and non-federal missions, this strategy will support whole-of-nation and partnership initiatives to protect against cyber threats to the United States and enable cyber resiliency.

The National Guard in the Cyberspace Landscape

The National Guard is building 59 cyber units across the 54 States, Territories, and the District of Columbia. The units align with the Army and Air Force and train in accordance with United States Cyber Command joint cyberspace training and certification standards.[1] These units are in varying stages of operational readiness, working alongside their service counterparts to execute training plans and fully operationalize the Total Force for the cyber mission. By the end of fiscal year 2019, the National Guard will have more than 3,700 Soldiers and Airmen associated with cyber units. These forces will continue to be used as both part of the United States Cyber Command Cyber Mission Force, the Department of Defense's operational force for addressing cyber threats, as well as in support of service and state requirements to protect relevant systems in cyberspace.

Domestically, the National Guard engages with Federal, State, Local, Tribal, and Territorial governments, and critical infrastructure owners and operators to provide cybersecurity support in local communities in the cyber defense of the homeland. One of the National Guard's distinguishing elements is the unique relationships that the thousands of members maintain with the local community and industry partners. These relationships are crucial during incident response and domestic support for both physical and cyber related activities.

Internationally, the National Guard provides cyber forces to enhance theater security cooperation through the State Partnership Program and other Combatant Command partner engagement programs. The State Partnership Program allows states to build long lasting and sustainable bonds with our foreign partners. Similarly, in times of crises, these enduring relationships and familiarity benefit when the Department of Defense is called upon to support contingencies around the world. Figure 1 describes National Guard cyber engagements tied to the three-core missions: warfight, homeland, and partnerships.

[1] 57 units does not include the Defensive Cyberspace Operations Elements

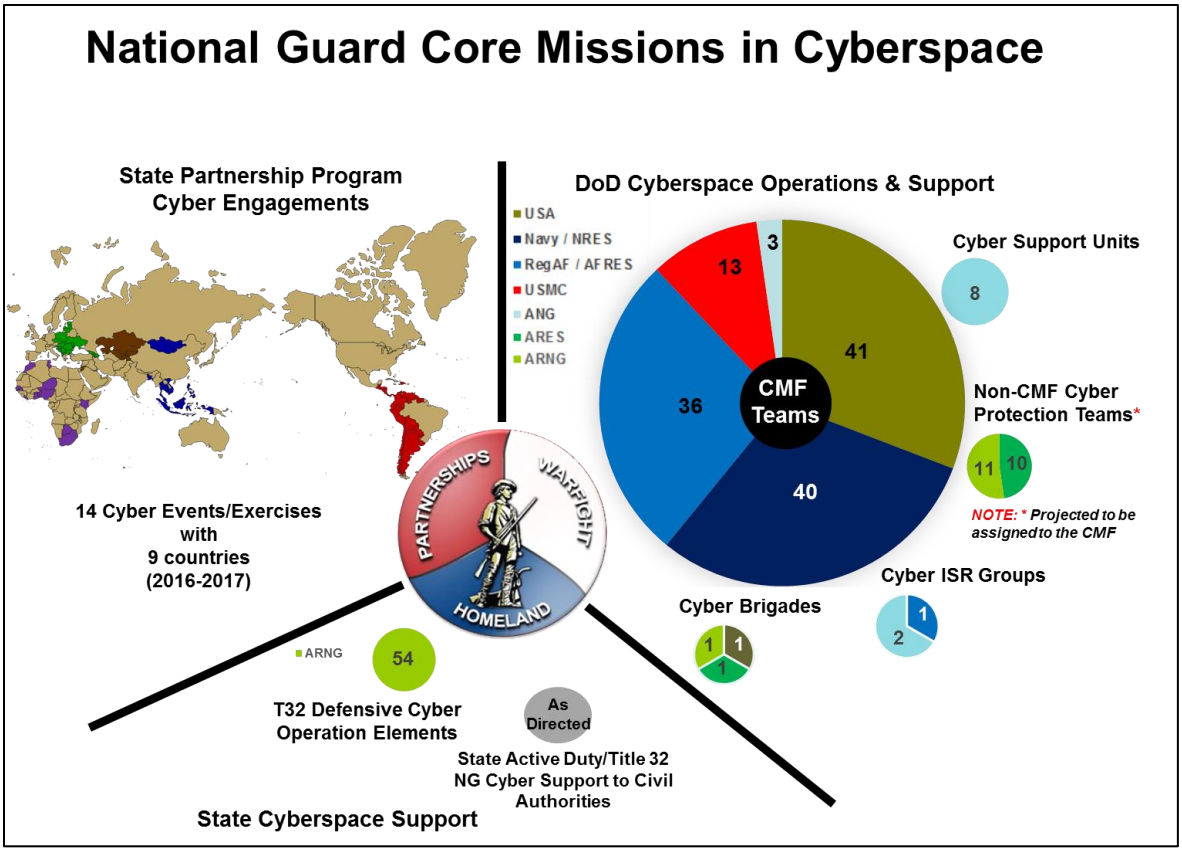


Figure 1. National Guard Core Missions in Cyberspace (Sept 2017)

Air National Guard Cyber Forces

The Air National Guard is building 15 Cyberspace Operations Squadrons; twelve fielding Cyber Protection Teams, and three sourcing personnel to a National Mission Team. Each Cyber Protection Team serves United States Cyber Command's Cyber Mission Forces on a rotational basis, ensuring an enduring presence of two teams. The three Cyberspace Operations Squadrons contributing to the National Mission Team each field two 22-person teams. These six teams will also mobilize on a 1:5 mobilization to dwell ratio as part of the United States Cyber Command Cyber Mission Force. Additionally, the Air National Guard has seven Cyber Intelligence, Surveillance, and Reconnaissance units. When assigned to an organization with the requisite authorities, these Cyber Intelligence, Surveillance, and Reconnaissance units provide cyber analytical efforts through digital network intelligence, analysis of adversary, air, space & cyber domains through signals intelligence development, post-collection (off-net) analysis of digital network intelligence data, and cyber threat discovery activities. Finally, the Air National Guard is also developing Mission Defense Teams designed to pair communication and intelligence personnel together to defend mission systems at each Wing. The Air National Guard established several other types of units in support of cyber operations to include training, operational support, and test and evaluation. (See Annex D for a listing of all Air and Army National Guard Cyber units and locations.)

Army National Guard Cyber Forces

In September 2017, the Army National Guard activated a Cyber Brigade; building units across multiple states to organize and modernize Army National Guard cyber forces in support of immediate and enduring Army, USCYBERCOM, and other Joint operation requirements. This construct allows for better preparation for incident response through synchronized training and sharing of best practices across states with limited resources; enabling 17 states to have Army National Guard cyber capabilities. The Army National Guard cyber units will fall under the 91st Cyber Brigade for training and readiness oversight, training standardization, and capabilities of all subordinate units. The brigade includes five battalions headquartered in the following states: Virginia (2), Massachusetts, South Carolina, and one state to be announced. Each operationally capable battalion consists of a Cyber Security Company, a Cyber Warfare Company, and the alignment of two Cyber Protection Teams. The Army National Guard Cyber Protection Teams are projected to be operational by the end of FY2022. Although not yet finalized, the Army National Guard expects to integrate the cyber protection teams into the United States Cyber Command Cyber Mission Force. These eleven cyber protection teams will operate on a 1:4 mobilization to dwell ratio, activated for one year and dwell for four years. Additionally, the Army National Guard maintains other cyber support elements such as Defensive Cyberspace Operations Elements and elements within the two Theater Information Operations Groups. (See Annex D for a listing of all Air and Army National Guard Cyber units and locations.)

The Army National Guard provides 54 Defensive Cyberspace Operations Elements in each of the States, Territories and the District of Columbia. In accordance with the Defensive Cyberspace Operations Elements Concept of Operations, the teams are comprised of up to ten traditional, part-time positions with the primary responsibility of defending GuardNet, a part of the Department of Defense Information Network, as well as other missions assigned by the Adjutants General. Defensive Cyberspace Operations Elements provide a cyber incident response capability to assist the Adjutant General and mission partners in defending key terrain in cyberspace. As some states are still developing their Defensive Cyberspace Operations Elements, the National Guard will work to ensure each state maintains access to cyber capabilities as needed. The support may be through the Emergency Management Assistance Compact process, similar to other civil support capabilities. These compacts serve as a complement to the federal disaster response system, providing timely and cost-effective relief to states requesting assistance. (See Annex D for a listing of all Air and Army National Guard Defensive Cyberspace Operations Elements units and locations.)

National Guard Authorities

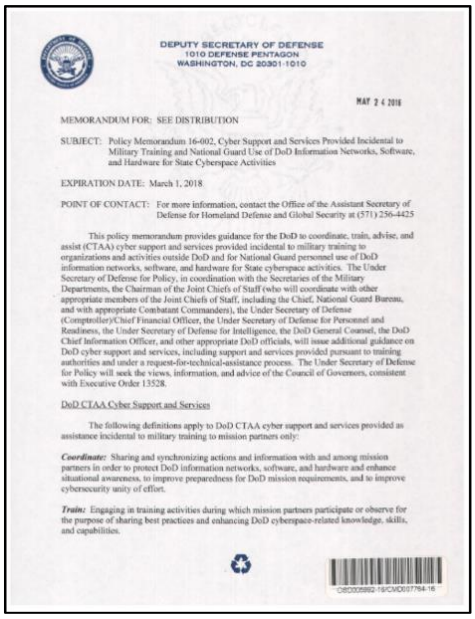
The National Guard provides forces for the warfight and assists cyber response and hygiene efforts by leveraging military cyber professionals in a variety of legal authorities. Under Title 10, United States Code authority (Title 10), National Guard personnel perform federal missions, usually through USCYBERCOM or their parent service, in accordance with the same rules, regulations and authority as their regular active component service counterparts. National Guard personnel can perform duties under state control in State Active Duty or Title 32, United States Code authority (Title 32). Individual states fund State Active Duty and personnel follow state statute and policy. Alternatively, under Title 32, the Governor, with President or Secretary of Defense approval, may activate Guardsmen to support homeland defense activities and defense support of civil authorities, which can include cyber defense and incident response activities.

The National Guard leverages its capabilities and authorities to support a variety of cyber missions across federal, state, and local levels. When mobilized into federal service, National Guard cyber Service members perform duties assigned by Joint Force Commanders or their parent military services. National Guard cyber forces also operate under state direction, as determined by their respective state authorities (State Active Duty or Title 32) and, when necessary, in support of operations or missions undertaken by the member's unit at the request of the President or Secretary of Defense under Title 32. When activated or operating in a non-federalized capacity, the National Guard will focus on protecting and defending state networks or systems and engage in Cybersecurity activities with critical infrastructure partners in accordance with applicable law and policy.

The federal government is investing resources in a variety of initiatives that build a framework for responding to cyber incidents as well as establishing programs that will keep the United States at the forefront of technology and innovation. Milestone achievements in 2016 included the Cybersecurity National Action Plan, Presidential Policy Directive 41, and the supporting National Cyber Incident Response Plan. These documents include a variety of actions integrating the National Guard into the domestic whole-of-nation cyber preparedness and response framework. Further, the Department of Defense Cyber Strategy incorporates the National Guard's role to coordinate, train, advise and assist federal, state and local agencies to provide support to law enforcement, homeland defense, and defense support of civil authorities activities in support of national objectives.

Existing Department of Defense Cyber Policies Affecting the National Guard.

Over the last few years, the National Guard has worked closely with policy makers in the Office of the Secretary of Defense, the Department of Homeland Security, United States Northern Command, and United States Cyber Command, among others, to establish policy depicting the National Guard's unique dual-use roles. These policies include Department of Defense Policy Memorandum 16-002, "Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information, Networks, Software and Hardware for State Cyberspace Activities," 24 May 2016, (aka "Coordinate, Train, Advise, and Assist Memo" (Figure 2)) and DoD Directive Type Memorandum (DTM) 17-007 "Interim Policy and Guidance for Defense Support to Cyber Incident Response," 21 June 2017.



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 2 4 2016

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Policy Memorandum 16-002, Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities

EXPIRATION DATE: March 1, 2018

POINT OF CONTACT: For more information, contact the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security at (571) 256-4425

This policy memorandum provides guidance for the DoD to coordinate, train, advise, and assist (CTAA) cyber support and services provided incidental to military training to organizations and activities outside DoD and for National Guard personnel use of DoD information networks, software, and hardware for State cyberspace activities. The Under Secretary of Defense for Policy, in coordination with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff (who will coordinate with other appropriate members of the Joint Chiefs of Staff, including the Chief, National Guard Bureau, and with appropriate Combatant Commanders), the Under Secretary of Defense (Comptroller)/Chief Financial Officer, the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Intelligence, the DoD General Counsel, the DoD Chief Information Officer, and other appropriate DoD officials, will issue additional guidance on DoD cyber support and services, including support and services provided pursuant to training authorities and under a request-for-technical-assistance process. The Under Secretary of Defense for Policy will seek the views, information, and advice of the Council of Governors, consistent with Executive Order 13528.

DoD CTAA Cyber Support and Services

The following definitions apply to DoD CTAA cyber support and services provided as assistance incidental to military training to mission partners only:

Coordinate: Sharing and synchronizing actions and information with and among mission partners in order to protect DoD information networks, software, and hardware and enhance situational awareness, to improve preparedness for DoD mission requirements, and to improve cybersecurity unity of effort.

Train: Engaging in training activities during which mission partners participate or observe for the purpose of sharing best practices and enhancing DoD cyberspace-related knowledge, skills, and capabilities.

Figure 2. CTAA Memo

The Coordinate, Train, Advise, and Assist document defines activities that the National Guard may conduct in support of organizations outside of Department of Defense, and provides parameters for use of Department of Defense information networks, software, and hardware for state cyberspace activities. Coordinate, Train, Advise, and Assist cyber support and services do not include offensive cyberspace operations or defensive cyberspace operations-response actions. This memo expires 1 March 2018, therefore requires a subsequent policy or directive providing similar authority. Further, the DoD Directive Type Memorandum (DTM) 17-007 – Interim Policy and Guidance for Defense Support to Cyber

Incident Response of 21 Jun 2017 supplements Department of Defense Directive 3025.18, provides procedures and assigns responsibilities regarding Defense Support to Cyber Incident Response (DSCIR). National Guard Bureau staff worked with staff in the Office of the Secretary of Defense to ensure this policy did not restrict or alter previously permitted activities provided by the 2016 CTAA memo. The 2017 policy does affect other military forces and requires that a DSCIR request must come to military forces or the Department of Defense from a lead federal agency as opposed to just a civil authority.

Response to Cyber Events.

Presidential Policy Directive-41 directed the development of the National Cyber Incident Response Plan to address cybersecurity risks and coordinate activities to mitigate, respond to, and recover from cyber incidents. The National Cyber Incident Response Plan describes the federal Government, the private sector, and State, Local, Tribal, and Territorial governments' various roles and responsibilities in cyber incidents and how the United States will organize its activities to manage significant cyber incidents. This Plan also leverages National Preparedness System policy to articulate how the Nation responds to and recovers from cyber incidents. This alignment with the National Preparedness System also allows cyber incident response to integrate seamlessly with physical incident response in cases where cyber incidents have physical impacts or vice versa.

As part of Presidential Policy Directive-41, the Cyber Incident Security Schema (Figure 3) defines cyber incident threat levels. A Significant Cyber event is an incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. In the event of a significant cyber event, as defined by Presidential Policy Directive-41, the Department of Homeland Security and Federal Bureau of Investigation are the lead federal agencies for events that occur outside of the Department of Defense information network. These organizations may submit requests for assistance from Department of Defense forces in accordance with United States Government and Department of Defense policies. When a lead federal agency requests Department of Defense cyber support, the requesting Combatant Command in coordination with the military service components, will determine the most appropriate response force; which may include National Guard personnel in a Title 10 or Title 32 status. The unique authorities and dual-use nature of the National Guard create opportunities for innovative approaches to protecting the homeland and integrating with Federal, State, Local, Tribal, and Territorial partners enabling a whole-of-nation approach to protecting cyberspace.

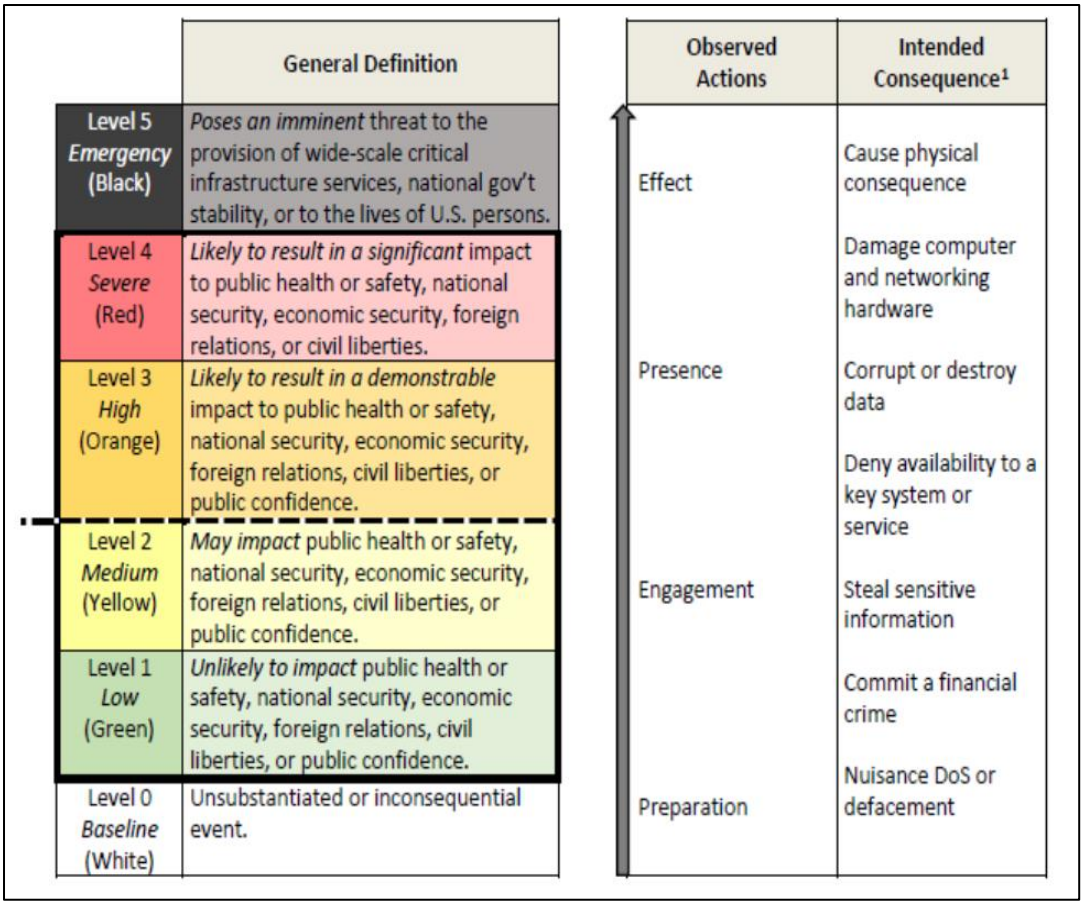


Figure 3. PPD-41 Cyber Incident Security Schema

Strategic Goals

The National Guard's cyber goals align with the National Guard's three-core missions – Fight America's Wars, Secure the Homeland, and Build Partnerships. These goals provide the foundation for the National Guard's whole-of-nation approach to cyber support.

Strategic Goal 1: Support the warfight by building and fully integrating National Guard cyber units into the operational federal mission.

Warfight Mission

The National Guard provides ready forces to the Army and Air Force capable of fighting in an array of complex environments, including cyberspace. As such, the National Guard will maintain properly manned, trained, and equipped cyber units available for prompt mobilization for federal missions and national emergencies. To achieve the warfight goal, National Guard cyber forces will integrate through common training and performance standards with service, combatant, and functional command force structures to meet current and emerging requirements.

Strategic Goal 1:

Support the warfight by building and fully integrating National Guard cyber units into the operational federal mission.

Objectives:

Maintain properly manned, trained, and equipped units

Continuously develop the cyber workforce

Enhance and expand warfighting capabilities through civilian acquired skills

As the National Guard cyber enterprise fields additional operational capability, the National Guard Bureau safeguards continuity of knowledge and readiness, providing a consistent presentation of highly trained forces for federal missions. Integral to United States Cyber Command Cyber Mission Forces, the National Guard Cyber Mission Force teams' integration and readiness is indiscernible from that of an active duty team. As an example, the National Guard Bureau ensures cyber forces have access to United States Cyber Command's Persistent Cyber Training Environment, providing the same training, tools, opportunities, and tactics, techniques and procedures align with the active component and leveraged across all teams. Further, the capturing and sharing of observations (lessons learned and best practices) from cyber exercises and real world events will assist National Guard cyber teams to improve and educate themselves and other military service components. As resources change and advance, the National Guard will work to ensure units continue to train and exercise to active component standards with the appropriate tools and resources, while National Guard members continue to gain experience through their civilian occupations.

Additionally, the National Guard will continue to develop the cyber workforce to ensure highly skilled, experienced Soldiers and Airmen are available for the warfight through innovative incentives, unique training opportunities, and attractive options to keep transitioning active component personnel in the cyber fight.

> *We will continue to build cyber forces, leveraging civilian acquired skills, to support the warfight. We will standardize our domestic cyber response capabilities for the homeland and refine our tactics, techniques and procedures to coordinate, train, advise, and assist mission partners as directed by the Governors.*

The National Guard will seek opportunities to leverage civilian acquired skills to enhance and expand warfighting capabilities. One such initiative is to become a center of excellence for Industrial Control System protection. The National Guard will build upon the schoolhouse and training

curriculum designed by the Washington Air National Guard to prepare cyber operators that defend critical Industrial Control System assets within the Department of Defense. Through partnership with the active component, the National Guard assists in the development of a key warfighting skillset also useful for Defense Support of Civil Authorities.

Strategic Goal 2: Protect the Homeland by providing highly trained cyber forces available to support Mission Partner requirements.

Homeland Federal, State, Local, Tribal, and Territorial Missions.

The National Guard is well postured to use its people, capabilities, and dual status authorities to assist the whole-of-nation effort in protecting United States infrastructure and responding to cyber incidents as directed. Guardsmen reside in thousands of communities across the United States and maintain enduring relationships with local businesses as unit members spend most of their careers in one location versus our active duty counterparts who move frequently. The longevity of National Guard personnel develops trust among community partners and creates opportunities otherwise not available to the Department of Defense. Further, the training our members receive as part of the federal mission coupled with the expertise gained through civilian employment offer unique capabilities for a Governor to use to help protect the local communities' population, infrastructure, and other critical national security assets susceptible to cyber aggression. National Guard members can serve in a Title 10, Title 32 or State Active Duty status. Title 32 and State Active Duty personnel are less restricted by the Posse Comitatus Act, which enables coordination with and support to law enforcement agencies. These unique National Guard characteristics facilitate a whole-of–nation proactive Cybersecurity posture and "first military responder" cyber incident response capability, helping the Nation achieve unity of effort in its cyberspace activities in the homeland.

The Council of Governors / Department of Defense Joint Action Plan on State-Federal Unity of Effort on Cybersecurity, dated July 2014, provides a framework and foundation for cybersecurity efforts in the homeland. The Cyber Joint Action

Strategic Goal 2:

Protect the Homeland by providing highly trained cyber forces available to support Mission Partner requirements

Objectives:

Facilitate information sharing, enhance communication and collaboration, enable shared situational awareness, and response capabilities among mission partners

Work with federal agencies to support and improve cybersecurity and resiliency in the homeland

Continue to engage and integrate with state mission partners to secure and defend cyberspace

Work with the Office of the Secretary of Defense and Congress to support cyber policy and legislation to better utilize our unique authorities and capabilities to execute federal and non-federal missions

Plan describes, "A *collaborative environment for states, territories, and the federal government to expedite and enhance the nation's response to cyber incidents . . . secure and defend cyberspace, including state and federal owned or operated critical infrastructure and key resources, in accordance with existing state and federal laws and policies."* In pursuing our homeland goal, the National Guard will continue to build upon the principles identified in the framework.

The National Guard currently coordinates with the Department of Homeland Security National Cybersecurity and Communications Integration Center to provide situational awareness to states on cyber incidents potentially affecting the homeland. This relationship allows the National Guard to facilitate further identification of threats to National Guard networks and coordinate actions with state governments and local officials within applicable laws and policies. To protect the homeland, the National Guard will pursue additional areas to facilitate information sharing, enhance communication and collaboration during cyber events, enable shared situational awareness, and share response capabilities among our Mission Partners.

The National Guard Bureau will work with federal agencies such as the Department of Defense, Department of Homeland Security, Department of Justice, and the Department of Energy, to identify, develop, and prioritize other areas the National Guard can support and improve cybersecurity and resiliency in the homeland. Cybersecurity activities include proactive components such as cyber hygiene and vulnerability assessments whereas cyber resiliency helps mitigate the effects of and speeds the recovery from cyber incidents and/or attacks. These types of actions contribute to a whole-of-nation approach to protecting cyberspace. Further, the National Guard will facilitate engagements between federal and state agencies as a method to address cyber vulnerabilities and incidents at the lowest level to help prevent a cascading event necessitating a national level response.

National Guard units across the 54 States, Territories, and District of Columbia will continue to engage and integrate with state mission partners to secure and defend cyberspace to protect our Nation's critical infrastructure. Today National Guard units around the country are engaging with state officials to integrate relevant assets into state Emergency response plans. States, including Washington, Michigan, Rhode Island, and Maryland, among many others, created cyber annexes to their state emergency response plans. As the likelihood of cyber-attacks increase, other states are likely to incorporate cyber-incident response roles for the National Guard into state all-hazards support plans. As the National Guard integrates into state emergency response plans, the policies and procedures will also need to be exercised. Additionally, states are beginning to use their cyber assets to perform cyber vulnerability assessments, secure state networks, and reduce the risk of cyber incidents. These proactive efforts address basic cyber hygiene actions, such as software updates, asset inventory, and drafting/auditing system security plans. As a result, the relationships built during these engagements will further enable and enhance the National Guard's ability to routinely, rapidly employ capabilities, improve the Nation's cybersecurity, and respond in the event of a cyber incident.

The National Guard has a long and successful history of using its federally trained, warfighting capabilities as the Department of Defense's first military responders supporting civil authorities during natural disasters and other domestic incidents. The National Guard provides assistance to states and local law enforcement through activities such as the National Guard Counter Drug program to address criminal and threat networks who leverage cyberspace to facilitate distributed but traditional illicit

activities. Although the National Guard strives to operate in cyberspace, the same as it does in the other domains, future cyber-related policies and/or legislation may need to be modified or clarified to ensure Department of Defense and the states can use the National Guard to its full potential in supporting mission partners in the homeland.

The National Guard Bureau will work with Congress, at the request of Congressional staffers, regarding legislation possibly affecting the National Guard. The National Guard Bureau will work with the Office of the Secretary of Defense to clarify and develop cyber policy to better utilize our unique authorities and capabilities to execute federal and non-federal missions in support of the Department of Defense, governors, and mission partners. The National Guard will expand and enhance the depth and quality of dialogue events to ensure all parties are aware of the value of the National Guard as an integral contributor to the nation's Cybersecurity in both state and federal duty statuses. Specific focus areas for policy dialogues will include, but are not limited to, how the Department of Defense and Governors could employ a Dual Status Commander in an event with a significant cyber component as well as how the National Guard can provide ongoing domestic intelligence support to law enforcement organizations within all applicable laws and policies. A key component to ensure the National Guard operates within all existing and future policies will be to develop proper training and procedures. Working in conjunction with Department of Defense and other relevant partners, the National Guard will develop or integrate any required unique training and procedures to help National Guard cyber forces contribute to the cybersecurity mission.

Strategic Goal 3: Expand and leverage enduring relationships with the Private Sector, Academia and International partners.

The National Guard creates, expands, and leverages partnerships at home and abroad to improve cyber resiliency, collaboration, shared situational awareness and response capabilities. Guardsmen distributed throughout the United States build relationships within the communities that they live and work. These regionally unique relationships are essential for building partnerships that are capable of leveraging appropriate cyber talent and experience. The partnerships, especially with critical infrastructure, will help bolster the Nation's Cybersecurity.

Strategic Goal 3:

Expand and leverage enduring relationships with the Private Sector, Academia and International partnerships

Objectives:

Pursue local and regional engagements with public and private sector mission partners

Expand international partnerships to build cybersecurity capacity in and protect against shared cyberspace threats

Partner with academia on mutually-beneficial education, training and research opportunities

Public and Private Sector.

The majority of America's information technology and computer systems are privately owned or operated by public sector entities at the state and local level. As a way to build partnership capacity in Cybersecurity, the National Guard will pursue local and regional engagements with public and private sector mission partners, particularly those that promote cyber hygiene, support critical local and regional government's network infrastructure, and facilitate the sharing of threat information to enhance collective cyber defense. A current partnership example is the Washington National Guard's participation in the annual Partners in Emergency Preparedness Conference, where in 2017, they co-led a "Community Cybersecurity" panel of state and private partners. Discussion topics for the panel focused on integrating efforts within the state's Comprehensive Emergency Management Plan and recognizing the public safety aspect of cybersecurity was not isolated organizationally, or only within government, but instead a community issue. Another example is the Ohio Cyber Collaboration Committee, an Ohio initiative bringing together over 100 local organizations across public, private, and academia including high schools and below. Designed to provide an environment for collaboration, Ohio Cyber Collaboration Committee gathers key stakeholders to strengthen cybersecurity for all in Ohio. Outreach to non-governmental and private sector organizations is critical in order to create a whole-of-nation approach to our Nation's Cybersecurity.

International Partnerships.

The National Guard State Partnership Program has been successfully building relationships for over 25 years that now includes 73 unique security partnerships involving 80 nations around the globe. Through State Partnership Program, the National Guard conducts military-to-military engagements in support of defense security goals but also leverages whole-of-society relationships and capabilities to facilitate broader interagency and corollary engagements spanning military, government, economic and social spheres. The National Guard will expand upon these relationships to include cyber engagements as another way to build partnership capacity in cybersecurity and protect against shared cyberspace threats. Additionally, the National Guard maintains relationships with foreign partners, outside of State Partnership Program in coordination with Department of Defense and the Department of State that would benefit from cyber integration. In 2016, the National Guard engaged with nine international partners on cyber related topics. Increasing international cyber engagements, including exercises, cyber subject matters expert exchanges, and cybersecurity awareness and education, will lay the foundation for a global cyber cooperation and shared situational awareness.

Academia Partnerships.

The National Guard will continue to partner with academia, to include increased participation in mutually beneficial education opportunities, research, training on cyber-ranges, and conducting vulnerability assessments. The National Guard is actively reaching out and developing partnerships with academia to expand and enhance training capabilities, develop sustainable pipelines of capable cyber operators for all sectors, and to leverage research and support to both cyber defense and inherently secure systems development. One relationship-building example with academia is the Texas Air National Guard's recent partnership with the University of Texas at San Antonio to develop timely and relevant Cybersecurity training tailored for National Guard senior leaders. Started in 2015, this course provides attendees an understanding of oversight issues, risk management, as well as policy and legal issues related to executive decision-making guiding National Guard cyberspace units. Another example includes Rhode Island working with the Pell Center at Salve Regina University to pursue an effort

focused on leadership at small and medium sized businesses to increase understanding of cybersecurity measures and solutions. Collaborating with academia enhances cyber knowledge, enables innovative problem solving, enriches training and creates a well-rounded, capable cyber force.

Implementing the Strategy

Achieving the goals and objectives outlined in National Guard Cyber Strategy requires a clear structure with a strategic implementation plan and an expectation of revision based on a rapidly changing environment. The National Guard Cyber Strategic plan is a companion to the National Guard Cyber Strategy that more clearly defines the specific ways and means used to achieve the strategic goals and objectives. The ways and means are broadly broken down into four lines of effort in the Plan: Workforce Development, Training and Exercises, Outreach, and Policy. Within the four lines of effort, Offices of Primary Responsibilities will identify specific initiatives that the Joint Force Headquarters-States can use to enable them to execute National Guard Cyber Strategy. America's ever increasing cyber dependencies coupled with the exponential escalation of technological and increasing threat sophistication has created an exceptionally dynamic domain demanding that the National Guard review the Cyber Strategy and Strategic Plan annually to ensure their relevancy.

Cyber General Officer Advisory Council: To ensure the maturation and fulfillment of the National Guard Cyber Strategy, the Chief of the National Guard Bureau designates the Cyber General Officer Advisory Council on National Guard Involvement in Cyberspace Activities as the primary coordination and advisory body for refining the strategy. The Chief of the National Guard Bureau appoints general officers from the National Guard Bureau Joint Staff, Army National Guard staff, Air National Guard staff, the Adjutants General, and other Department of Defense organizations where National Guard general officers are serving. The Cyber General Officer Advisory Council serves to manage the link between the National Guard Bureau and the Joint Force Headquarters-States and will facilitate the National Guard Cyber Strategy implementation by convening quarterly to review the National Guard Cyber Strategic Plan progress and provide advice and recommendations on strategic planning, resourcing and policy decisions. The National Guard Bureau Joint Cyberspace Operations Division will administer and coordinate Cyber General Officer Advisory Council forums.

National Guard Bureau-Joint Cyberspace Operations: The National Guard Bureau Domestic Operations and Force Development Directorate (NGB-J3/7), specifically the Cyberspace Operations Division (NGB-J36), will manage the National Guard Cyber Strategy and National Guard Cyber Strategic Plan execution. In addition, the National Guard Bureau-Joint Cyberspace Operations is the principle staff division that synchronizes Army National Guard and Air National Guard cyber policy to ensure alignment with the National Guard Cyber Strategy. It leads the collaboration of the National Guard Cyber Strategy and National Guard Cyber Strategic Plan with the Strategic Plans, Policy and International Affairs Directorate (NGB-J5), Joint Forces Headquarters-States, Department of Defense, Department of Homeland Security and Department of Justice/Federal Bureau of Investigation. National Guard Bureau-Joint Cyberspace Operations is the primary National Guard cyber representative with interagency and intergovernmental entities for efforts to enhance our cyber domain awareness capability and improve reporting processes between NGB-J3/7, Joint Force Headquarters-States, and other mission partners.

Conclusion

The Chief of the National Guard Bureau has directed a build-assess-build approach for National Guard cyber forces to ensure the National Guard is strengthening critical cyberspace capabilities and capacity with an emphasis on meeting the requirements of a whole-of-nation response. The National Guard Cyber Strategy and Strategic Plan enables National Guard cyber forces development and use by following four lines of effort that flow across three-core missions: "Fight America's Wars, Secure the Homeland, and Build Partnerships." By simultaneously identifying and working toward both short and long term initiatives, the National Guard is able to progress and continually asses its capabilities.

Within the next three years, we will successfully integrate National Guard cyber organizations at both state and federal levels to ensure whole-of-nation prevention, protection, and response posture to a cyber incident. As a community-based force, National Guard personnel build lifelong relationships leading to unique partnerships and additional capabilities to protect the homeland. To ensure the National Guard fully capitalizes on the citizen Soldiers' inherent strengths, these cyber-partner engagements must capitalize on the National Guard's unique titles/authorities that facilitate enduring relationships with their local communities, state and municipal governments, and their own civilian employers. Fully aware and experienced with regards to the legal boundaries of their engagements, National Guard cyber forces operate under any status without increasing risk to the mission; bringing capacity to respond to cyber emergencies in unity with our public, private, and local partners.

The National Guard will continue to be a well-trained and equipped cyber force that enables the Army and Air Force to meet mission requirements at home and abroad. Guardsmen will accomplish this by leveraging civilian acquired skills in conjunction with meeting United States Cyber Command joint training standards and working collaboratively with the military services, Federal, State, Local, Tribal, and Territorial agencies, and the private sector. Postured to defend the United States homeland and vital interests from disruptive or destructive cyber-attacks, and able to aid Federal, State, Local, Tribal, Territorial and mission partners when properly tasked, the National Guard is "Always Ready, Always There."

Annex A: References and Authorities

The references listed below are just a small portion of the vast landscape of documentation and legislation in which the National Guard operates. While this lists federal authorities, certain critical infrastructure sectors are under various sector regulations as outlined by law.

This list is not exhaustive, but leveraged as a foundational resource.

- 10 U.S.C. – Armed Forces
- 18 U.S.C. – Crimes and Criminal Procedure
- 32 U.S.C. – National Guard
- Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience
- Presidential Policy Directive (PPD)-8: National Preparedness
- Presidential Policy Directive (PPD)-41: U.S. Cyber Incident Coordination Policy
- Cybersecurity Act of 2015 (P.L. 114-213)
- National Cybersecurity Protection Act of 2014 (P.L. 113-282)
- Presidential Executive Order (PEO) – Commission on Enhancing National Cybersecurity of 9 February 2016
- National Defense Strategy
- The National Military Strategy of the United States of America of 2016
- National Security Strategy of February 2015
- Department of Defense Cyber Strategy of April 2015
- National Defense Authorization Act (NDAA) 14 Sec 933 of H.R. 3304
- Chief National Guard Bureau, GSLC of February 2016
- NGB Strategic Direction to the National Guard of June 2013
- Chief of the National Guard Bureau (CNGB) Vision for the Future 2017
- National Cyber Incident Response Plan (NCIRP), December 2016
- Department of Defense Policy Memorandum 16-002, Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information, Networks, Software and Hardware for State Cyberspace Activities (aka “Coordinate, Train, Advise, and Assist Memo”, 24 May 2016)
- DoD Directive Type Memorandum (DTM) 17-007 – Interim Policy and Guidance for Defense Support to Cyber Incident Response, 21 June 2017
- Army National Guard Cyber Strategy of 2016
- Air Force Information Dominance Flight Plan
- Executive Order (EO) 13800: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure of 11 May 2017
- The Army Cyberspace Strategy for Unified Land Operations 2025, January 2016
- 2018 National Guard Bureau Posture Statement: Building a Force for the Future
- United States Cyber Command Joint Cyberspace Training & Cert Standards (JCT&CS), Feb 2012
- Cybersecurity National Action Plan (CNAP), 09 February 2016
- National Guard Cyber Capabilities Based Assessment Final Report, 24 March 2016
- Joint Requirements Oversight Memorandum (JROCM) 073-14
- Council of Governors / Department of Defense Joint Action Plan on State-Federal Unity of Effort on Cybersecurity, July 2014

Annex B: Acronyms

ANG	Air National Guard
ARNG	Army National Guard
CTAA	Coordinate, Train, Advise and Assist
PPD	Presidential Policy Directive
SLTT	State, Local, Tribal, and Territorial
USCYBERCOM	United States Cyber Command

Annex C: Definitions

Term	Definition
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev 1
Advise	Providing advice to mission partners that aids in the development of potential strategies, plans, and solutions for preventing, protecting, and defending against, responding to, mitigating the effects of, and recovering from cyber incidents. Coordinate, Train, Advise, and Assist Memo, May 2016
Agency	Any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include - (i) the General Accounting Office; (ii) Federal Election Commission; (iii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (iv) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. Title 44 United States Code (U.S.C.), Sec. 3502
Assist	Supporting mission partners in their prevention of, protect ion against, mitigation against, and recovery from a cyber incident. CTAA Memo, May 2016
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. Committee on National Security Systems Instruction (CNSSI) No. 4009, April 6, 2015
Command of National Guard Forces	Governors serve as commanders-in-chief of their respective state's National Guard forces. As the only military force that a governor can call upon to respond to disasters and other emergencies, the National Guard serves as a critical resource in emergency response and can quickly provide much-needed capabilities. The National Guard also serves as an operational force supporting overseas missions alongside the nation's active duty forces. National Governors Association website
Coordinate	Sharing and synchronizing actions and information with and among mission partners in order to protect Department of Defense information networks, software, and hardware and enhance situational awareness, to improve preparedness for Department of Defense

	mission requirements and to improve cybersecurity unity of effort. CTAA Memo, May 2016
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters. CNSSI No. 4009, April 6, 2015
Cyber Exercise	A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption. National Cyber Security Division (NCSD) Glossary, DHS Homeland Security Exercise and Evaluation Program
Cyber Incident	An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. PPD-41
Cyber Mission Force (CMF)	The Cyber Mission Force currently comprises about 6,000 individuals across the 133 teams. The focus of USCYBERCOM's Cyber Mission Force teams aligns with the Department of Defense Cyber Strategy's three primary missions: Defend Department of Defense networks and ensure their data is held secure; support joint military commander objectives; and, when directed, defend U.S. critical infrastructure. U.S. Cyber Command News Release 24 OCT 16
Cyber Protection Team (CPT)	CPTs augment traditional defensive measures and defend priority Department of Defense networks and systems against priority threats. Department of Defense Cyber Strategy
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. NSPD-54/Homeland Security Presidential Directive (HSPD)-23
Cyberspace	The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. NSPD-54/HSPD-23

Cyberspace Operations	The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Department of Defense Joint Publication (JP) 3-0
Cyberspace Situational Awareness	Cyberspace Situational Awareness (SA) is the requisite current and predictive knowledge of cyberspace and the OE (operational environment) upon which CO (cyberspace operations) depend, including all factors affecting friendly and adversary cyberspace forces. JP 3-12R
Defense Support of Civil Authorities (DSCA)	Support provided by U.S. federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense Component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected states, elects and requests to use those forces in Title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. Department of Defense Directive 3025.18
Defensive Cyberspace Operations (DCO)	Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. JP 3-12
Department of Defense Information Networks (DoDIN)	The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called DODIN. (JP 6-0)
Dwell	That period of time between the release from active duty pursuant to sections 12301(a), 12302, 12304, 12304a, and 12304b of 10 U.S.C. and the reporting date for a subsequent tour of such active duty. Such time includes any active duty performed in accordance with sections 12301(b) and 12301(d) of 10 U.S.C. between such two periods of active duty pursuant to sections 12301(a), 12302, 12304, 12304a, and 12304b of 10 U.S.C.. Department of Defense Instruction (DoDI) 1235.12
Emergency Management Assistance Compact (EMAC)	This compact provides for mutual assistance between the states entering into this compact in managing any emergency disaster that is duly declared by the Governor of the affected state, whether arising from natural disaster, technological hazard, man-

	made disaster, civil emergency aspects of resources shortages, community disorders, insurgency, or enemy attack. Public Law 104–321
Federal Agency	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. NIST SP 800-37 Rev 1
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization's information systems(s). NIST SP 800-34 Rev 1
Industrial Control System	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). NIST SP 800-82 Rev 1
Interoperability	The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. JP 6-0
Key Resource	A publicly or privately controlled asset necessary to sustain continuity of government and/or economic operations, or an asset that is of great historical significance. National Cyber Security Division (NCSD) glossary
Mission Partners	Those with which the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government, state and local governments, non governmental organizations, and the private sector. CTAA Memo, May 2016
National Guard	The National Guard is part of the Reserve Components of the U.S. Armed Forces and consists of both Army and Air National Guard.
National Mission Team (NMT)	NMTs will defend the United States and its interests against cyberattacks of significant consequence. Department of Defense Cyber Strategy

Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. NIST SP 800-53 Rev 4
Offensive Cyberspace Operations	Cyberspace operations intended to project power by the application of force in or through cyberspace. JP 3-12
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. CNSSI No. 4009, April 6, 2015
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. PPD-21
Significant Cyber Incident	A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. PPD-41
State Active Duty (SAD)	The Governor can activate National Guard personnel to "State Active Duty" in response to natural or man-made disasters or Homeland Defense missions. SAD is based on state statue and policy as well as state funds. Soldiers and Airmen remain under the command and control of the Governor. National Guard Association of the United States (NGAUS) Fact Sheet
State Partnership Program (SPP)	A Department of Defense security cooperation program consisting of all State Partnerships authorized by Section 1205 of P.L. 113-66, as amended, under which programs of activities of members of the National Guard of a state or territory and the military forces, or security forces, or other government organizations (but only those with primary functions that include disaster response or emergency response) of a foreign country may be established. Department of Defense Instruction 5111.20
Supervisory Control and Data Acquisition (SCADA)	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that

	must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. NIST SP 800-82 Rev 1
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. NIST SP 800-30 Rev 1
Train	Engaging in training activities during which mission partners participate or observe for the purpose of sharing best practices and enhancing Department of Defense cyberspace-related knowledge, skills, and capabilities. CTAA Memo, May 2016
US-CERT (United States Computer Emergency Readiness Team)	A partnership between the Department of Homeland Security (DHS) and the public and private sectors, established to protect the nation's internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation. NIST SP 800-53 Rev 4
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. NIST SP 800-30 Rev 1
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. CNSSI No. 4009, April 6, 2015

Annex D: National Guard Cyber Units

ARNG Cyber Forces

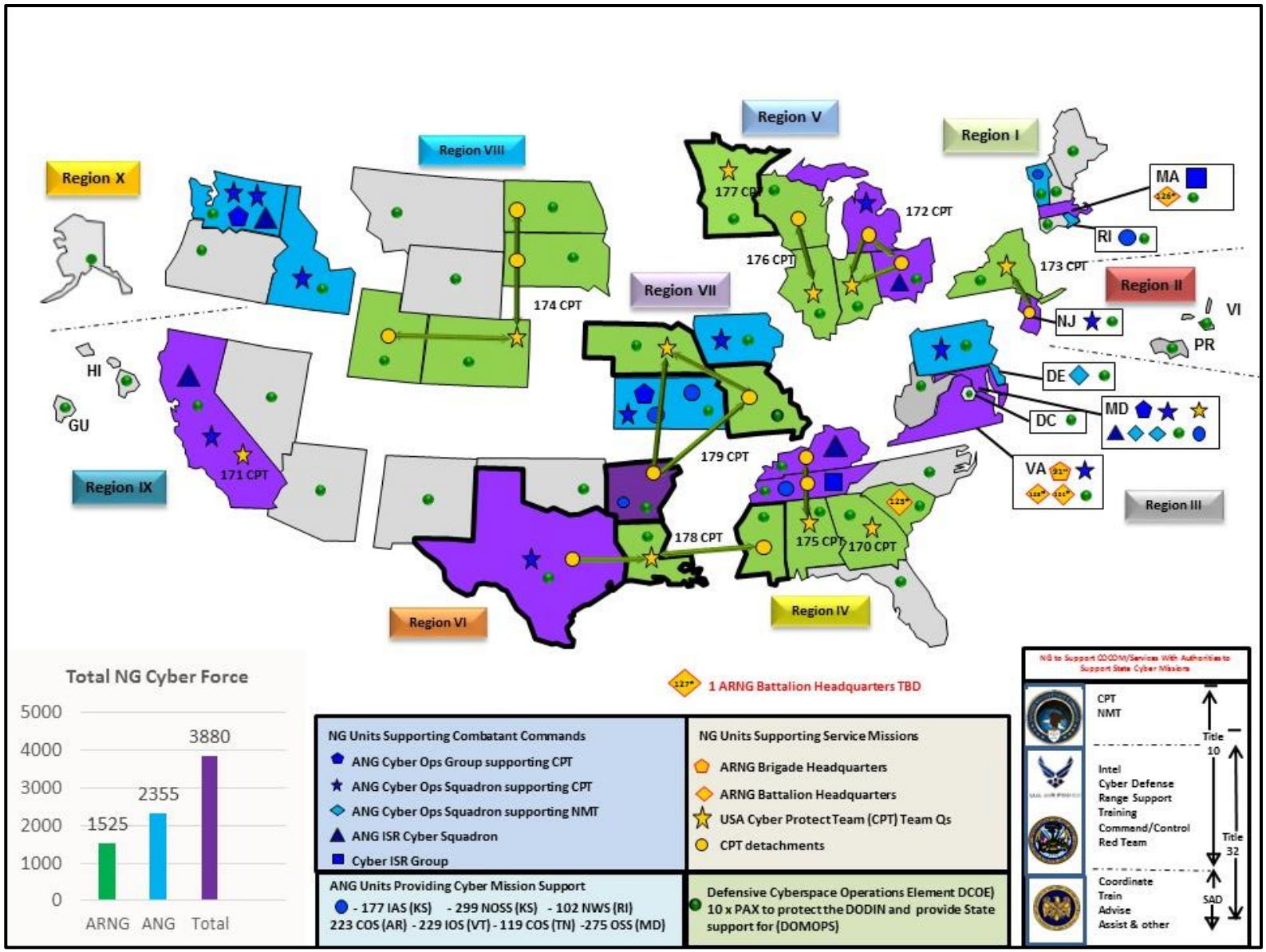
State	FEMA Region	Unit Type	CPT Affiliation	Interstate Partnership	City/Base	# PAX	CMF?
AL	4	Cyber Protection Team	TM 175	**AL**/KY/TN	Decatur	11	No
AR	6	Cyber Protection Team	TM 179	**NE**/MO/AR	Camp Robinson	7	No
CA	9	Cyber Protection Team	TM 171	**CA**	Mather AFB	39	No
CO	8	Cyber Protection Team	TM 174	**CO**/ND/SD/UT	Buckley AFB	11	No
GA	4	Cyber Protection Team	TM 170	**GA**	Fort Gillam	39	No
IL	5	Cyber Protection Team	TM 176	**IL**/WI	Fort Sheridan	18	No
IN	5	Cyber Protection Team	TM 172	**IN**/MI/OH	Indianapolis	11	No
KY	4	Cyber Protection Team	TM 175	**AL**/KY/TN	Frankfort	14	No
LA	6	Cyber Protection Team	TM 178	**LA**/TX/MS	Camp Jackson	14	No
MA	1	Cyber Battalion HQ	126 CPB			26	
MA	1	Cyber Security Company	136 CSC			36	
MA	1	Cyber Warfare Company	146 CWC			33	
MD	3	Cyber Protection Team	TM 169	**MD**	Linthicum	39	No
MI	5	Cyber Protection Team	TM 172	**IN**/MI/OH	Battle Creek	14	No
MN	5	Cyber Protection Team	TM 177	**MN**	Minneapolis	39	No
MO	7	Cyber Protection Team	TM 179	**NE**/MO/AR	Jefferson City	21	No
MS	4	Cyber Protection Team	TM 178	**LA**/TX/MS	Camp McCain	7	No
ND	8	Cyber Protection Team	TM 174	**CO**/ND/SD/UT	Bismarck	7	No
NE	7	Cyber Protection Team	TM 179	**NE**/MO/AR	Lincoln	11	No
NJ	2	Cyber Protection Team	TM 173	**NY**/NJ	McGuire-Dix-Lakehurst	14	No
NY	2	Cyber Protection Team	TM 173	**NY**/NJ	Latham	25	No
OH	5	Cyber Protection Team	TM 172	**IN**/MI/OH	Columbus	14	No
SC	3	Cyber Battalion HQ	125 CPB			26	
SC	3	Cyber Security Company	135 CSC			36	
SC	3	Cyber Warfare Company	145 CWC			33	
SD	8	Cyber Protection Team	TM 174	**CO**/ND/SD/UT	Rapid City	7	No
TN	4	Cyber Protection Team	TM 175	**AL**/KY/TN	Nashville	14	No
TX	6	Cyber Protection Team	TM 178	**LA**/MS/TX	San Antonio	18	No
UT	8	Cyber Protection Team	TM 174	**CO**/ND/SD/UT	Draper	14	No
VA	3	Cyber Brigade HQ	91 BDE		Ft Belvoir	81	No
VA	3	Cyber Battalion HQ	123 CPB		Ft Belvoir	26	
VA	3	Cyber Security Company	133 CSC		Ft Belvoir	36	
VA	3	Cyber Warfare Company	143 CWC		Ft Belvoir	33	
VA	3	Cyber Battalion HQ	124 CPB		Ft Belvoir	26	
VA	3	Cyber Security Company	134 CSC		Ft Belvoir	36	
VA	3	Cyber Warfare Company	144 CWC		Ft Belvoir	33	
WI	5	Cyber Protection Team	TM 176	**IL**/WI	Madison	21	No
TBD		Cyber Battalion HQ	127 CPB			26	
TBD		Cyber Security Company	137 CSC			36	
TBD		Cyber Warfare Company	147 CWC			33	

States with Army and Air Cyber Units – AR, CA, KY, MA, MD, MI, NJ, OH, TN, TX, VA

ANG Cyber Forces

State	FEMA Region	Unit Type	CPT Affiliation	City/Base	# PAX	CMF?
AR	6	Cyber Mission Support (TNG)	223 CTS	Little Rock AFB	27	No
CA	9	Cyber ISR Squadron	149 IS	Mather AFB	71	No
CA	9	Squadron Supporting CPT	261 COS	Sepulveda ANG Station	71	Yes
DE	3	Squadron Supporting CPT	166 COS	New Castle	71	Yes
IA	7	Squadron Supporting CPT	168 COS	Des Moines	71	Yes
ID	10	Squadron Supporting CPT	224 COS	Gowen Field	71	Yes
KS	7	Cyber Mission Support	177 IAS	McConnell AFB	71	No
KS	7	Cyber Mission Support	299 NOSS	McConnell AFB	71	No
KS	7	Squadron Supporting CPT	127 COS	McConnell AFB	71	Yes
KS	7	Cyber Ops Group	184 COG	McConnell AFB	30	
KY	4	Cyber ISR Flight	223 IF	Louisville	16	No
MA	1	Cyber ISR Group	102 ISRG	Otis ANGB	206	No
MD	3	Cyber ISR Squadron	135 IS	Martin State	71	No
MD	3	Cyber Ops Group	175 COG	Warfield ANGB	18	No
MD	3	Cyber Mission Support	275 OSS	Warfield ANGB	53	No
MD	3	Squadron Supporting CPT	275 COS	Warfield ANGB	71	Yes
MD	3	Squadron Supporting NMT	175 COS	Warfield ANGB	71	Yes
MD	3	Squadron Supporting NMT	276 COS	Warfield ANGB	71	Yes
MI	5	Squadron Supporting CPT	272 COS	Battle Creek ANGB	71	Yes
NJ	2	Squadron Supporting CPT	140 COS	McGuire-Dix-Lakehurst	71	Yes
OH	5	Cyber ISR Squadron	124 IS	Springfield-Beckley ANGB	71	No
PA	3	Squadron Supporting CPT	112 COS	Willow Grove	71	Yes
RI	1	Cyber Mission Support	102 COS	Quonset ANGB	71	No
TN	4	Cyber ISR Group	218 ISRG	Nashville	206	No
TN	4	Cyber Mission Support	119 COS	McGhee Tyson ANGB	142	No
TX	6	Squadron Supporting CPT	273 COS	Kelly AFB	71	Yes
VA	3	Squadron Supporting CPT	185 COS	JB Langley-Eustis	71	Yes
VT	1	Cyber Mission Support (TNG)	229 IOS	Northfield	35	No
WA	10	Cyber ISR Squadron	256 IS	Fairchild AFB	71	No
WA	10	Cyber Ops Group	252 COG	Camp Murray ANG Station	30	No
WA	10	Squadron Supporting CPT	143 COS	Camp Murray ANG Station	71	Yes
WA	10	Squadron Supporting CPT	262 COS	JB Lewis-McCord	101	Yes

States with Army and Air Cyber Units – AR, CA, KY, MA, MD, MI, NJ, OH, TN, TX, VA


Region X
Region VIII
Region V
Region I
Region VII
Region II
Region IX
Region VI
Region IV
Region III
177 CPT
172 CPT
176 CPT
174 CPT
173 CPT
179 CPT
171 CPT
178 CPT
175 CPT
170 CPT
MA
RI
NJ
VI
PR
DE
MD
DC
VA
HI
GU
Total NG Cyber Force
5000
4000
3000
2000
1000
0
1525
2355
3880
ARNG
ANG
Total
1 ARNG Battalion Headquarters TBD
NG Units Supporting Combatant Commands
ANG Cyber Ops Group supporting CPT
ANG Cyber Ops Squadron supporting CPT
ANG Cyber Ops Squadron supporting NMT
ANG ISR Cyber Squadron
Cyber ISR Group
NG Units Supporting Service Missions
ARNG Brigade Headquarters
ARNG Battalion Headquarters
USA Cyber Protect Team (CPT) Team Qs
CPT detachments
ANG Units Providing Cyber Mission Support
- 177 IAS (KS) - 299 NOSS (KS) - 102 NWS (RI)
223 COS (AR) - 229 IOS (VT) - 119 COS (TN) -275 OSS (MD)
Defensive Cyberspace Operations Element DCOE)
10 x PAX to protect the DODIN and provide State support for (DOMOPS)
CPT
NMT
Title 10
Intel
Cyber Defense
Range Support
Training
Command/Control
Red Team
Title 32
Coordinate
Train
Advise
Assist & other
SAD