Cyber Incident Annex

Coordinating Agency

Mississippi Department of Information Technology Systems (ITS)

Support Agencies

Mississippi Department of Public Safety (MDPS)
- Office of Homeland Security (MOHS)
- Mississippi Analysis and Information Center (MSAIC)
- Mississippi Cyber Unit (MCU)

Mississippi Emergency Management Agency (MEMA)
Mississippi Military Department (MMD)
- Mississippi National Guard (MSNG)
  - Defensive Cyberspace Operation Element (DCOE)
  - Detachment 2, Cyber Protection Team 178 (DET 2, CPT 178)

All Other State Agencies, Departments, and Commissions

Federal Coordinating Agency

Department of Homeland Security (DHS)
- Cyber and Infrastructure Security Agency (CISA)

Department of Justice (DOJ)
Department of Defense (DOD)
- United States Cyber Command (USCYBERCOM)

Federal Cooperating Agencies

Department of Energy (DOE)
Department of Homeland Security (DHS)
Department of State (DOS)
Department of Transportation (DOT)
Department of the Treasury (USDT)
Intelligence Community
National Institute of Standards and Technology (NIST)
Office of Management and Budget (OMB)

This page left blank intentionally.

Table of Contents

Cyber Incident Annex

1. INTRODUCTION.

a. Purpose. Cybersecurity incidents can potentially cause a significant disruption of government operations and Critical Infrastructure and Key Resources (CIKR). Addressing cyber incidents may require a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recover from the incident. The purpose of this Annex is to identify resources, policies, organizations, actions pre-incident, during, and following a cyber-incident, responsibilities, federal support, and maintenance of this Annex.

b. Scope. This Annex describes the framework for state agency coordination of response and recovery activities related to cybersecurity incidents impacting state and local government data systems, networks, and critical infrastructure. This Annex is not intended to replace state agency plans and procedures. The Cyber Incident Annex is built primarily upon the National Cyber Incident Response Plan (NCIRP). The NCIRP describes a national approach to cyber incidents, delineating the critical role of private sector entities, local, state, and tribal governments, and multiple federal agencies in responding to incidents and how those activities fit together. State agencies are responsible for implementing their agency-specific cybersecurity incident response plans, policies, and procedures.

The coordination with the federal government during a cybersecurity incident is dynamic and shaped by the nature of the event. The complexity of creating a framework for addressing all possible scenarios resulting from a cybersecurity incident would severely limit its effectiveness. This framework intends to address broad concepts focused on Mississippi's interface with several key federal departments, including:

(1) Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA);

(2) DHS/Office of Intelligence and Analysis (I&A);

(3) DHS/U.S. Secret Service (USSS);

(4) U.S. Department of Justice (DOJ)/Federal Bureau of Investigation (FBI);

(5) U.S. Department of Defense (DOD);

Additionally, this framework is built on the premise that the following partners will work together to coordinate the actions necessary for the identification, information exchange, response, and

remediation to mitigate the damage caused by a cybersecurity event of statewide or national significance:

(6) Mississippi Department of Information Technology Services (ITS);

(7) Mississippi Department of Public Safety (MDPS)/Mississippi Office of Homeland Security (MOHS)

(8) MOHS/Mississippi Cyber Unit (MCU);

(9) MOHS/Mississippi Information and Analysis Center (MSAIC);

(10) Mississippi Emergency Management Agency (MEMA);

(11) Mississippi Military Department (MMD)/Mississippi National Guard (MSNG);

(12) Private and Public Sector Resources;

This framework may be utilized in any cybersecurity incident. Cybersecurity Incidents of State Significance include authoritative reports of severe cyber threats and disruptions targeting Mississippi's information and critical infrastructure. This infrastructure comprises the Internet, telecommunications networks, and critical infrastructure information systems. This Annex describes the specialized application of the Comprehensive Emergency Management Plan (CEMP) to cyber-related incidents. Cyber-related Incidents of State Significance may activate both Emergency Support Function (ESF) #2 (Communications) and the Cyber Incident Annex.

2. RELATIONSHIP TO WHOLE COMMUNITY. This section describes how state cyber incident responders relate to other elements of the whole community. Basic concepts that apply to all members of the whole community include:

a. Local, Tribal, and State Governments.

(1) Gain situational awareness through reporting at each level: from local, state, and tribal governmental agencies, non-governmental organizations, industry essential service providers, other private sector partners, and residents. Information and support requests flow from the incident level to decision-makers through operations and coordination centers. At the same time, decision-makers and operations and coordination centers provide accurate, actionable, and relevant information to support incident operations.

(2) Initiate actions to save and sustain lives, reduce human suffering, and provide additional resources and assistance to response efforts. ESF #2 accomplishes this by stabilizing and re-establishing critical infrastructure quickly and efficiently, coordinating requests for additional support, identifying and integrating resources and capabilities, and coordinating information flow. Local authorities are responsible for obtaining required waivers and clearances related to ESF #2 support.

b. Private Sector/Non-Governmental Organizations. The private sector owns or operates most of the Nation's communications infrastructure and is a partner and/or lead for the rapid restoration of infrastructure-related services.

Through planning and coordination, private sector entities provide critical information for incident action planning and decision-making during an incident. Private sector mutual aid and assistance networks also facilitate sharing resources to support response.

3. POLICIES. State and federal government cyber security principles govern the procedures discussed in this Annex.

a. This Annex complements the National Plan for Telecommunications Support in NonWartime Emergencies, hereafter referred to as the National Telecommunications Support Plan (NTSP).

b. This Annex is implemented within the framework and operating principles of the CEMP, National Response Framework (NRF), MEMA Response Framework, and pursuant to the following references and authorities:

(1) National Security Act of 1947, as amended;

(2) The Defense Production Act of 1950, as amended;

(3) Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot ACT) Act Of 2001;

(4) Cybersecurity and Infrastructure Security Agency Act of 2018 (H.R. 3359, Pub.L. 115–278;

(5) Strengthening American Cybersecurity Act of 2022 (S.3600)

(6) The Enhancement of Non-Federal Cyber Security, The Homeland Security Act (Section 223 of Public Law [P.L.] 107-276);

(7) Section 706, Communications Act of 1934, as amended (47 U.S.C. 606);

(8) Federal Information Security Management Act (FISMA);

(9) Homeland Security Presidential Directive-5 (HSPD-5);

(10) Homeland Security Presidential Directive-7 (HSPD-7);

(11) Presidential Policy Directive 21: Critical Infrastructure Security and Resilience;

(12) The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets, 2003;

(13) The National Strategy for Homeland Security, 2007;

(14) Executive Order 12472: The Assignment of National Security Emergency Preparedness Responsibilities for Telecommunications;

(15) Executive Order 12333: United States Intelligence Activities, as amended;

(16) National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems;

(17) National Emergency Telecommunications Plan, September 2019;

(18) National Cyber Incident Response Plan, December 2017;

(19) Mississippi Code Annex § 25-53-201, Enterprise Security Program;

(20) Mississippi Code Annex § 25-61-11.2.

(21) Mississippi Code Annex § 33-15-11;

4. CONCEPT OF OPERATIONS. State responses to cyber incidents will be coordinated through MEMA, the MCU, and ITS to ensure proper funding and distribution of available resources.

A cyber-related Incident of State Significance may take many forms: an organized cyber-attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber

consequences, or other incidents capable of causing extensive damage to critical infrastructure or key assets, including local government information infrastructure.

Large-scale cyber incidents may overwhelm government and private-sector resources by disrupting the internet and/or taxing critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid identification, information exchange, investigation, and coordinated response and remediation often can mitigate the damage caused by this type of malicious cyberspace activity.

The State government plays a significant role in managing inter-governmental (federal, state, local, and tribal) and, where appropriate, public-private coordination in response to cyber incidents of State Significance. State government responsibilities include:

a. Providing indications and warning of potential threats, incidents, and attacks;

b. Information-sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation;

c. Analyzing cyber vulnerabilities, exploits, and attack methodologies;

d. Providing technical assistance;

e. Conducting investigations, forensics analysis, and prosecution;

f. Attributing the source of cyber-attacks;

g. Defending against the attack;

h. Leading state-level recovery efforts;

These activities are the product of and require a concerted effort by state and local governments and non-governmental entities such as private industry and academia. All cyber incidents within state agencies, local government, or any incident within the state with a legal notification/disclosure requirement will be reported to the MSAIC, also known as the State Fusion Center.

5. ORGANIZATION.

a. Federal. To assist in understanding the primary federal agencies that could play a part in addressing a cyber incident, the following organization descriptions are provided:

(1) Department of Homeland Security/Cybersecurity and Infrastructure Security Agency. DHS/CISA is a focal point for cyberspace security to analyze, warn, share information sharing, reduce vulnerability, mitigate, and aid national recovery efforts for critical infrastructure information systems. CISA facilitates interaction and collaboration (except for investigation and prosecution of cybercrime, military operations to defend the homeland, or other activities identified below) between and among the federal departments and agencies; state, local, tribal, and territorial governments (SLTT); critical infrastructure owners and operators; the private sector; and international organizations. Other federal departments and agencies with cyber expertise collaborate with and support DHS/CISA in accomplishing its mission. DHS/CISA is responsible for the preparation of and response to cyber threats, vulnerabilities, and incidents. The agency also works closely with SLTT and private sector partners in its prevention and protection role.

DHS/CISA also works closely with federal law enforcement agencies to investigate and prosecute threats to and attacks against cyberspace. As appropriate, DHS/CISA also reports to the Secretary of Homeland Security and the Executive Office of the President regarding coordination and response related to cyber incidents. DHS/CISA coordinates with the Department of State (DOS) to notify and resolve incidents with foreign governments. DHS and DOS coordinate with the inter-agency community to work with foreign countries and international organizations to strengthen the protection of U.S. critical information infrastructures and those foreign critical information infrastructures on which the United States relies.

(2) Department of Homeland Security/Office of Intelligence and Analysis. DHS I&A has assigned an Intelligence Officer (IO) with departmental and national intelligence authorities to Mississippi. DHS I&A is the primary medium to report national security and cyber threat intelligence concerns to the U.S. Intelligence Community and broader Federal Government for analysis and information sharing. As a DHS and the U.S. Intelligence Community (IC) member, the DHS IO is the senior intelligence official for DHS I&A and resides at the MSAIC.

(3) Department of Homeland Security/United States Secret Service. The DHS/USSS is authorized to investigate financially motivated cybercrime. This cybercrime can include electronic fund transfer frauds, access device frauds, ransomware, business e-mail compromise, network intrusion, false identification documents or devices, and any fraud or other criminal activity utilizing federally insured financial institutions. In 2001, Congress passed the Patriot Act and mandated the Secret Service to establish a nationwide Electronic Crimes Task Forces network to prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure financial payment systems.

In 2020, the Secret Service consolidated the Financial and Electronic Crimes Task Forces into 44 Cyber Fraud Task Forces to more efficiently and effectively combat cyber-enabled financial crimes. Cyber Fraud Task Forces (CFTF) have been established nationwide and overseas to

increase the resources, skills, and vision by which local, state, tribal, and federal law enforcement agencies team with prosecutors, private industry, and academia. The Secret Service Cyber Fraud Task Force partnership model facilitates incident response and allows the Secret Service to be a trusted resource to an organization for guidance during the initial stage of a cyber incident.

(4) Department of Justice/Federal Bureau of Investigation. While working with other law enforcement agencies, the DOJ and the FBI lead the national effort to investigate and prosecute cybercrime. The FBI uses its legal authorities and cyber resources to investigate, attribute, disrupt, and prosecute cyber intrusions of a criminal or national security origin. The DOJ and FBI work closely with the private sector to coordinate efforts, thwart, detect, and investigate cybercrime. The FBI also conducts domestic cyber threat intelligence collection, analysis, and dissemination. DOJ coordinates with the DHS to provide domestic investigative information relevant to the DHS analysis of the cyber infrastructure's vulnerability to a terrorist attack or the DHS analysis of terrorist threats against the cyber infrastructure.

(5) Department of Defense. United States Cyber Command (USCYBERCOM) is one of the eleven unified combatant commands of the DOD. It unifies the direction of cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters DOD's cyber expertise. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to:

(a) Direct the operations and defense of specified DOD information networks;

(b) Conduct full-spectrum military cyberspace operations to enable actions in all domains;

(c) Ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

b. State. To assist in understanding the principal state agencies addressing a cyber incident within Mississippi, the following organization descriptions are provided:

(1) Mississippi Department of Information Technology Service. ITS administers the Enterprise Security Program to execute the duties and responsibilities of Mississippi Code Ann. 25-53-201. ITS provides coordinated oversight of the cybersecurity efforts across all state agencies, including cybersecurity systems, services, policies, standards, and guidelines. ITS implements enterprise technology solutions and procedures capable of improving the cybersecurity posture in any agency, institution, or function of state government. Per the Program requirements, Mississippi state agencies must report all cybersecurity incidents to ITS. Reporting to ITS provides the ability to:

(a) Coordinate activities among agencies experiencing similar incidents to help identify and resolve the problem more quickly than if done separately.

(b) Implement appropriate controls in enterprise IT systems to reduce the likelihood of the cybersecurity incident impacting other state agencies.

(c) Share threat intelligence to help agencies protect themselves from similar attacks.

(d) Share information between public and private stakeholders and other appropriate entities. Collaborate with key entities that can provide the necessary cybersecurity expertise to assist when required.

(2) Mississippi Department of Public Safety/Mississippi Office of Homeland Security. MDPS/MOHS coordinates with federal, tribal, state, and local agencies during manmade and natural disasters and works to prevent, protect, and respond to threats and/or acts of terrorism, including cyber incidents within our state. MOHS leads the efforts in "All-Hazard" prevention, preparedness, and response by continuing to foster strong partnerships across professional response disciplines. The office educates the citizens of Mississippi through awareness and outreach efforts. These efforts are accomplished through training, equipping, and informing the populace about the steps necessary to keep themselves and their communities vigilant and prepared.

(3) Mississippi Office of Homeland Security/Mississippi Cyber Unit. The MCU will be the state's centralized cybersecurity information, threat, mitigation, incident reporting, and response center. The MCU comprises specialists who focus on cyber preparedness and response. The strategic plan for the MCU establishes the framework for generating tactical or operational intelligence, strategic threat intelligence, and advanced technical investigative support. The MCU manages the Cyber Threat Protection Program (CTPP). The CTPP is focused on hardening and improving the security of current networks and operating systems. Coordinate risk and threat assessments by sector and region. Develops and maintains sensors and honeypots across participating networks. Perform real-time threat sharing using industry-standard protocols. The CTPP will continue to build relationships with federal, state, and local partners. Additionally, the MCU will coordinate state and federal response to cyber incidents within Mississippi.

(4) Mississippi Office of Homeland Security/Mississippi Analysis and Information Center. MOHS/MSAIC maximizes Mississippi's law enforcement and public safety agency's ability to detect, prevent, apprehend, and respond to potential criminal and terrorist activities to support the all-crime, all-hazards, and all-threats approach intelligence. MSAIC serves as a nexus for information sharing among agencies in the public and private sectors.

(5) Mississippi Emergency Management Agency. The mission of MEMA is to safeguard Mississippi and its citizens by fostering a culture of preparedness, executing timely response during a disaster, and quickly restoring quality of life post-event. Emergency Management is a comprehensive approach to administering and governing mitigation, preparedness, response, and recovery efforts. Recognizing that emergency management begins and ends at the local level, MEMA is a vital asset for Mississippi. Regardless of the threat, MEMA will plan and prepare for emergency scenarios, respond to and support local EMAs during emergency events, and coordinate resource recovery efforts in the wake of a disaster.

(6) Mississippi Military Department. The MSNG operates two cyber teams: the Defensive Cyberspace Operation Element (DCOE) and Detachment 2, Cyber Protection Team 178 (DET 2, CPT 178). The DCOE and CPT provide defensive cyber capabilities and situational awareness to defend the National Guard Network. Additionally, they Conduct Defensive Cyberspace Operations (DCO) on military networks to support mission requirements identified by DOD or state leadership. In compliance with federal and state laws, DCO may be expanded to include cyber command readiness inspections, vulnerability assessments, cyber opposing force support, critical infrastructure assessments, theater security cooperation, Federal Emergency Management Agency support, training support, advisory, and assistance support. State-level cyber support can be conducted in any status for training purposes. All other support should be conducted in a State Active Duty status or in coordination with the Innovative Readiness Training (IRT) program.

6. ACTIONS.

a. Pre-Incident. ITS, MCU, MSAIC, MEMA, and the MSNG are key stakeholders in the State of Mississippi's pre-incident planning for cybersecurity incidents. Each agency is responsible for maintaining relationships and collaborating with their respective federal and tribal partners and other states, public, and private entities. The intent is to build relationships that leverage federal, tribal, state, and private sector capabilities.

Federal departments and agencies maintain computer incident response capabilities that can rapidly respond to cyber incidents on their networks, including prolonged events. Law enforcement, the Intelligence Community, and the DOD also maintain mechanisms that improve the Nation's readiness to address cyber incidents. The DOJ has a network of prosecutors trained in handling cybercrime. The FBI and the DHS/USSS have agents that specialize in high-tech investigations. Federal law enforcement's international cybercrime network and the relationships fostered with foreign countries allow them the opportunity to obtain electronic data and evidence.

b. Notification and Activation Procedures. The State of Mississippi leverages a cyber-threat schema closely aligned with federal and state schemas. The schema includes four alert-level protocols:

(1) GREEN or LOW indicates low risk.

(a) No unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity.

(b) It is unlikely to impact public health or safety, national/state security, economic security, civil liberties, or public confidence.

(2) YELLOW or MEDIUM indicates a significant risk due to increased hacking, viruses, or other malicious activity that compromises systems or diminishes service.

(a) At this level, known vulnerabilities are being exploited with moderate damage or disruption, or the potential for significant damage or disruption is high.

(b) It may impact public health or safety, national/state security, economic security, civil liberties, or public confidence.

(3) ORANGE or HIGH indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes numerous system compromises, or compromises critical infrastructure.

(a) At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.

(b) It will likely impact public health or safety, national/state security, economic security, civil liberties, or public confidence.

(4) RED or SEVERE indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

(a) At this level, vulnerabilities are exploited with severe or widespread damage or disruption of Critical Infrastructure Assets.

(b) It will likely severely impact critical infrastructure services, national/state security, economic security, and harm to individuals involving loss of life or serious life-threatening injuries.

c. Initial Actions. When a notification of a potential cybersecurity incident is received, key stakeholders of this Annex will take the following actions:

(1) Establish the facts and assumptions regarding the cybersecurity incident.

(2) Determine the appropriate threat level commensurate with the incident.

(3) Review the incident's size, scope, and potential statewide impact and recommend whether or not to activate this Annex.

If the Annex is activated, key stakeholders will:

(4) Notify appropriate federal, tribal, and local government stakeholders of the incident.

(5) Cooperatively assess the ongoing impact of the incident and provide an analysis of the extent and duration of the incident.

(6) Collaboratively work with federal, tribal, and local governments to recommend a prioritized set of actions to restore computer and network services during response and recovery operations.

(7) Provide incident reports to appropriate internal and external partners for situational awareness. Reports will contain an appropriate classification based on the type of incident, and the recipients must agree to observe the classification.

Cybersecurity incidents may not reach the threshold for activation of this Annex. In these cases, response to an incident is the responsibility of local/tribal government authorities and first responders. However, incident reporting is still required regardless of annex activation.

Cybersecurity incidents that require the state to declare an emergency/disaster and/or involve larger geographic areas (multiple states, regions, nationwide, international, or globally) may require the Federal government to declare a Presidential Declared Emergency/Disaster. Upon such a declaration, the Federal government will activate appropriate Annexes of the NRF, including the Cyber Incident Annex.

d. Ongoing Actions. Key stakeholders of this Annex will work collaboratively with appropriate partners (DHS, DOJ, FBI, etc.) to develop and maintain situational awareness of the cybersecurity domain.

DHS coordinates technical and other assistance with and/or to other federal agencies and, upon request, to the state, local, and tribal governments and the private sector for response to major failures of critical information systems.

7. CHALLENGES AND CONSIDERATIONS. The response to and recovery from a cyber-incident of State Significance must consider existing challenges to effectively managing significant cyber incidents and the resulting physical effects of such cyber incidents and cyber consequences of physical incidents. Such consideration allows resources to be appropriately channeled into resolving identified challenges. Identifiable challenges include:

a. Management of Multiple Cyber Events. The occurrence or threat of multiple cyber incidents may significantly hamper the ability of responders to manage the cyber incident adequately. Strategic planning and exercises should be conducted to assist in addressing this problem.

b. Availability and Security of Communications. A debilitating infrastructure attack could impede communications needed for coordinating response and recovery efforts. A secure, reliable communications system is required to enable public and private-sector entities to coordinate efforts if normal communications channels are inoperable.

c. Availability of Expertise and Surge Capacity. Federal agencies must ensure sufficient technical expertise is developed and maintained within the government to address the wide range of ongoing cyber-attacks and investigations. In addition, the ability to surge technical and analytical capabilities in response to cyber incidents that may occur over a prolonged period must be planned for, exercised, and maintained.

d. Coordination with the Private Sector. Cyberspace is primarily owned and operated by the private sector; therefore, the authority of the Federal government to exert control over activities in cyberspace is limited.

e. Coordination with Local Government. Unlike Mississippi state agencies, communication channels for the many local government sectors (K-12 schools, counties, cities, law enforcement, tribal, etc.) are not established. Communication channel(s) with local government sectors for cybersecurity incident notification should be established to facilitate response activities as outlined in this Annex.

8. RESPONSIBILITIES.

a. Federal Entities.

(1) Department of Homeland Security/Cyber and Infrastructure Security Agency. CISA's Cybersecurity Advisors (CSA) are the front-facing cyber experts supporting regional operations capabilities. CSAs are the liaison and focal point for communications, coordination, and outreach between CISA Headquarters (HQ), SLTT partners, the private sector, and other Federal partners. They promote cyber preparedness and resiliency, incident response, risk mitigation, situational awareness, and manage major cyber engagements, working towards cyber resilience for public and private sector partners. During cyber incidents, CSAs are the first point of contact for CISA and work with affected entities to ensure that CISA resources are appropriately notified of the incident and allocate resources to assist in remediation efforts.

(2) Department of Homeland Security/Office of Intelligence and Analysis. DHS I&A is responsible for collecting, reporting, analyzing, and disseminating intelligence information that fuses unique state and local information with IC information to answer Intelligence Community (IC) intelligence requirements, DHS information needs, and/or MSAIC Key Intelligence Questions (KIQs). During a cyber incident, the DHS IOs will respond as follows:

(a) DHS IO will receive notification of a cyber incident from the stakeholder and/or MSAIC to include all event details and Indicators of Compromise (IOCs).

(b) When reported cyber information meets a collection requirement, the DHS IO will draft a raw intelligence information report (IIR).

(c) DHS IO will share information with stakeholder partners and classified data with cleared stakeholder partners involved with the incident.

(d) DHS IO will provide Mississippi with any IC feedback or DHS HQ offer(s) of mitigation assistance or related intelligence information.

(e) Information not meeting an IC or DHS requirement will be referred to MSAIC and reported through the appropriate MSAIC information-sharing groups.

(3) Department of Homeland Security/United States Secret Service. DHS/USSS works with the FBI and other law enforcement agencies in helping to lead the national effort to investigate and prosecute cybercrime. USSS coordinates with DOJ to provide domestic investigative information used in the DHS analysis of the vulnerability of the cyber infrastructure to terrorist attacks.

(4) Department of Justice/Federal Bureau of Investigation. DOJ/FBI works with cyber security stakeholders and other law enforcement agencies in helping to lead the national effort to investigate and prosecute cybercrime. DOJ/FBI coordinates with cyber security stakeholders and other law enforcement agencies to provide domestic investigative information used in the DHS analysis of the vulnerability of the cyber infrastructure to terrorist attacks.

b. State Entities.

(1) Mississippi Information Technology Services. When ITS receives a report of a potential cybersecurity incident from a state agency, ITS coordinates with the affected agency to gather the facts and determine if the incident reaches the threshold of statewide importance. If it is determined that the incident could be of statewide significance, ITS will report the incident to the appropriate stakeholders and advise on initial actions as outlined in this Annex.

(2) Mississippi Office of Homeland Security. MOHS will work closely with our local, state, tribal, and federal partners to determine if there is a terrorism nexus relating to the cyber incident. MOHS will identify available resources and utilize partnerships as a force multiplier to prevent additional incidents. The MOHS will establish an ongoing exchange of information between the state and the CIKR sectors to support situational awareness as needed. The MOHS Public Information Officer (PIO) will work with our partner agencies to address information flow to and from the public and control potential misinformation on social media platforms.

(3) Mississippi Cyber Unit. MCU will collect, analyze, and disseminate real-time cyber intelligence information to operational and executive elements. MCU will support SLTT organizations through coordinated response and active cyber monitoring.

(4) Mississippi Information and Analysis Center. MSAIC will collect, analyze, and disseminate real-time criminal intelligence information to operational and executive elements. MSAIC will support intelligence-led policing and national security strategies and/or initiatives by analyzing and disseminating data collected across Mississippi, the continental United States, and its territories to support critical infrastructure protection.

(5) Mississippi Emergency Management Agency. MEMA is responsible for coordinating support for all disasters that affect the State of Mississippi.

(6) Mississippi Military Department. MMD maintains federally allocated cyber units for state and national-level mission requirements. Under state active duty or approved IRT orders, MMD may provide cyber response activities to state and local government agencies.

9. AUTHORITIES AND REFERENCES. In addition to the cyber security-specific authorities and references listed in section 3.b., the procedures in this Cyber Incident Annex are built on the core coordinating structures of the CEMP and references listed below. The specific responsibilities of each department and agency are described in the respective ESF, Support, and Incident Annexes, internal agency plans, policies, and procedures. See the CEMP Base Plan or the SEOC Operations Section for a comprehensive list of Authorities and References.

a. Robert T. Stafford Disaster Relief and Emergency Assistance Act; amended the Disaster Relief Act of 1974, PL 93-288.
https://www.fema.gov/sites/default/files/2020-03/stafford-act_2019.pdf

b. Public Law 98-473, Emergency Federal Law Enforcement Assistance Act, October 1984
https://uscode.house.gov/view.xhtml?path=/prelim@title34/subtitle5/chapter501&edition=prelim

c. United States Code, Title 18, Section 1385 (Posse Comitatus Act)
https://www.govinfo.gov/app/details/USCODE-2011-title18/USCODE-2011-title18-partI-chap67-sec1385

d. MS Code, Ann. § 33-15(1972): Mississippi Emergency Management Act of 1995, Title 33-15, et al. [Successor to Mississippi Emergency Management Law of 1980]
MS Code 33-15

e. MS Code, Ann. § 45-1-2(7): Public Safety and Good Order
MS Code 45-1

f. Homeland Security Presidential Directive 8 (HSPD-8) https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

g. National Incident Management System, Third Edition, October 2017
https://www.fema.gov/media-library/assets/documents/148019

h. National Preparedness System
https://www.fema.gov/emergency-managers/national-preparedness/system

i. National Response Framework, Fourth Edition, October 2019
https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf

j. National Protection Framework, Second Edition, June 2016
https://www.fema.gov/sites/default/files/2020-04/National_Protection_Framework2ndjune2016.pdf

k. National Prevention Framework, Second Edition, June 2016
https://www.fema.gov/sites/default/files/2020-04/National_Prevention_Framework2ndjune2016.pdf

l. MEMA Response Framework, June 2023
MEMA Downloads/MEMA Publications

The MEMA reference repository, containing the CEMP base plan, associated annexes, appendices, and other supporting documents, can be found at MEMA Downloads.

Most Mississippi emergency management stakeholders have access to the MEMA Downloads site. However, non-registered stakeholders may access the repository by submitting an e-mail request to preparedness@mema.ms.gov.

10. REVIEW AND MAINTENANCE. This Annex will be continuously reviewed and exercised to evaluate the state's and political subdivisions' ability to execute response and recovery operations and support tribal, local, and municipal emergency management agencies. Directors of primary state agencies are responsible for maintaining internal policies, plans, SOPs, checklists, and resource data to ensure a prompt and effective response to a disaster in support of this Annex. For training purposes and exercises, the MEMA Executive Director may activate this Annex as deemed necessary to ensure high operational readiness.

MEMA will revise this Annex on a biennial basis. The revision will include testing, reviewing, and updating the document and its procedures. This Annex will be updated every two years, or as necessary, to incorporate new presidential or state directives, legislative changes, and procedural changes based on lessons learned from exercises and actual incidents. This Annex will be rewritten every four (4) years.

MEMA coordinates updates, modifications, and changes to the Annex. Heads of state agencies with ESF coordinator responsibility will periodically provide information regarding changes with available resources, personnel, and operating procedures. Recommended changes will be submitted to MEMA for approval and distribution. Submit recommendations via e-mail to preparedness@mema.ms.gov.

This Annex applies to all state agencies, state boards, state commissions, and state departments assigned emergency responsibilities and to all elements of local government in accordance with current law and Executive Orders (EOs).