MARSH RISK CONSULTING

RISK. DISPUTES. STRATEGY.

Setting the Standard in the Cyber Maelstrom

The Cyber Challenge for Public Agencies

February 26, 2016
Indian Wells

maelstrom | ‘māl,sträm |
noun
a situation of confused movement or violent turmoil

Thomas A. Fuhrman
Managing Director
Marsh Risk Consulting

MARSH

The Takeaway Message

- Sophisticated cyber attackers are at work.
- California state, county, and city agencies have a *fourfold* cybersecurity challenge:
  - Protecting the security of private citizen data.
  - Preserving the online availability and integrity of state services.
  - Guiding and supporting citizens and businesses in cybersecurity.
  - Responding to cyber incidents affecting California.
- All levels of government – federal, state, tribal, county, and city – must work together to protect against and respond to cyber intrusions.

Setting the Standard in the Cyber Maelstrom
The Cyber Challenge for Public Agencies

Outline

- **The State OF Cybersecurity Today**
- **The State AND Cybersecurity Today**
- **Working Together in Cyber: State and Federal**
- ***Cyber Emergency!* A Crisis Scenario**

The Cyber Threat Today

The Threat:	Those who deliberately intrude into networks and IT systems to conduct unauthorized or unlawful activities.
Professional	• Technically very advanced with refined tradecraft. • Well-organized and well-funded, often by nation-states (military, foreign intelligence services), organized crime, or other organizations.
Capitalists	• Everything has a price – often in virtual currency. • Advanced tools openly available on the internet. • First to market with differentiated offerings wins.
Elusive	• Operate in the Dark Web in forums and IRC chat rooms. • Understand anonymity, legal jurisdictions, and internet architecture. • Exploit differences in laws from country to country.

Is the threat 10 feet tall?

What Can Hackers Do?

Hackers can…

- Interrupt or corrupt online operations (e.g., interfere with agency missions and delivery of citizen services).
- Use IT infrastructure as an entry point to the networks of other entities.
- Gain access to voice or video teleconferences.
- Capture (and sell) PHI and PII held by agency systems on California residents.
- Exfiltrate sensitive or proprietary data (e.g., business applications and reports, legal documents).
- Make servers and end user machines part of a botnet for cyber crime.
- Exploit IT infrastructure to attain anonymity in other illicit cyber activities.
- Gain control of your email accounts.
- Increasingly capable of physical damage and destruction.

Hackers are just as interested in government systems and data as they are commercial.

The Functional Pieces of Cybersecurity

IDENTIFY — The organizational understanding to manage cybersecurity risks.

PROTECT — Develop and implement safeguards to ensure delivery of critical infrastructure services.

DETECT — Develop and implement activities to identify the occurrence of cybersecurity events.

RESPOND — Develop and implement activities to take action on cybersecurity events.

RECOVER — Maintain plans for resilience and restore capabilities or services after a cybersecurity event.

Source: NIST Cybersecurity Framework

Security "controls" – technical, administrative-physical – are implemented to mitigate risk.

Cybersecurity in the Real World

Some Realities

- Most enterprises are not as secure as they should be:
  - Securing networks and data is a difficult proposition.
  - Coordinating security with IT.
  - Building and managing the controls environment to support policy.
  - Trying to keep up with the dynamics.
  - Increasingly close relationship between risk manager and risk transfer.
- Many/most enterprises still have a foot on square one: asset identification.
- Technology is necessary but not sufficient.
- Heavy reliance on third-party providers increases exposure in two ways:
  - Business disruption due to a cyber event at the service provider.
  - Intrusions that exploited cyber weaknesses at the third party and migrated to the primary network.

Conditions or Degrees of Emergency

State of War Emergency

- … California or nation is attacked by an enemy of the United States, or upon receipt of a warning from the federal government that such an attack is probable or imminent…

State of Emergency

- … conditions of extreme peril to the safety of persons and property within the state caused by such conditions as air pollution, fire, flood, storm, epidemic, riot, drought, sudden and severe energy shortage, plant or animal infestation or disease… earthquake or volcanic prediction…

Local Emergency

- … conditions of extreme peril to the safety of persons and property within the territorial limits of a county, city and county, or city… beyond the control of the services, personnel, equipment, and facilities of that political subdivision and require the combined forces of other political subdivisions…

Source: State Code §8558, California Emergency Services Act

Can a cyber incident rise to the level of emergency?

Challenges and Responsibilities in Cyber

The state has long recognized its responsibility to mitigate the effects of natural, manmade, or war-caused emergencies which result in conditions of disaster or in extreme peril to life, property, and the resources of the state, and generally to protect the health and safety and preserve the lives and property of the people of the state.

—California Emergency Services Act

- The *fourfold* cybersecurity challenge to California state, county, and city agencies:
  - Protecting the security of private data of California's 38 million people *(pursuant to HIPAA and California State Law).*
  - Preserving the online availability and integrity of state services *(pursuant to Continuity of Operations/ Continuity of Government requirements).*
  - Guiding and supporting citizens and businesses in cybersecurity *(pursuant to State Constitution of California).*
  - Responding to cyber incidents affecting California.

Setting the Standard in the Cyber Maelstrom
The Cyber Challenge for Public Agencies

Outline

- **The State OF Cybersecurity Today**
- **The State AND Cybersecurity Today**
- **Working Together in Cyber: State and Federal**
- ***Cyber Emergency!* A Crisis Scenario**

California Cyber Resources and Missions

Resource	*Plan/ Strategize*	*Assess/ Prevent*	*Train/ Exercise*	*Respond*	*Coordinate*
State of California Emergency Plan	✘				
Governor's Office of Emergency Services	✘	✘	✘	✘	✘
California Information Security Office	✘	✘			
California State Threat Assessment Center (STAC)		✘			
California Military Department	✘	✘	✘	✘	✘
California Cybersecurity Integration Center (Cal-CSIC)					✘
Multi-State Information Sharing and Analysis Center (MS-ISAC)	✘	✘		✘	✘
Cybersecurity Task Force					✘
Council of Governors	✘				✘

See Annex A for more detail

Setting the Standard in the Cyber Maelstrom
The Cyber Challenge for Public Agencies

Outline

- **The State OF Cybersecurity Today**
- **The State AND Cybersecurity Today**
- **Working Together in Cyber: State and Federal**
- ***Cyber Emergency!* A Crisis Scenario**

Federal Government Cyber Resources and Missions

Resource	*Plan/ Strategize*	*Assess/ Prevent*	*Train/ Exercise*	*Respond*	*Coordinate*
Department of Homeland Security	✘	✘	✘	✘	✘
Department of Defense	✘	✘	✘	✘	✘
Federal Bureau of Investigation		✘	✘	✘	✘
National Security Agency		✘	✘	✘	✘
Federal Emergency Management Agency (FEMA)				✘	✘
National Institute of Standards and Technology	*Research, standards, and guidance.*				

Note: The missions and jurisdictions of federal agencies in the identified functional areas are prescribed by law. Operationalizing these functions may require authorities invoked by appropriate presidential declarations.

See Annex B for more detail

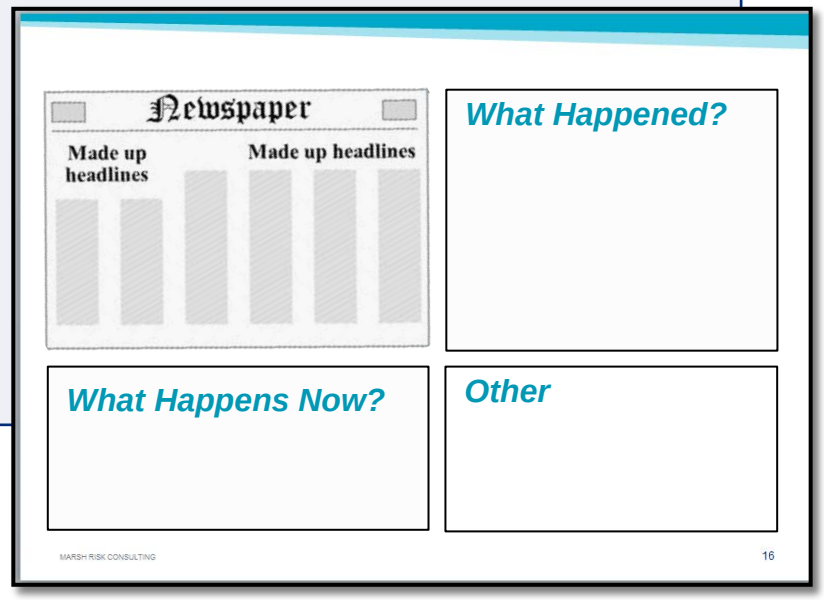
Setting the Standard in the Cyber Maelstrom
The Cyber Challenge for Public Agencies

Outline

- **The State OF Cybersecurity Today**
- **The State AND Cybersecurity Today**
- **Working Together in Cyber: State and Federal**
- ***Cyber Emergency!* A Crisis Scenario**

The Scenario Concept

- These scenarios portray a hypothetical series of events to examine organizational response.
- The likelihood of these events occurring is not a consideration, only the plausibility.
- Most of the elements of these scenarios are draw from previous real-world incidents.
- The purpose of this discussion is to elucidate:
  - The role of state and federal agencies as currently organized and aligned.
  - The challenges of making decisions in a complex crisis environment.
  - Insights that can be applied in risk management.



Format for scenario slides

Yesterday

All Times PST


THE WALL STREET JOURNAL.

What's News

Cyber Hack Shuts Markets

SEC Acts as NASDAQ, NYSE hit

SIMULATED

Cyber Exposure of Stock Exchanges Increases Despite Years of Effort

Declining Revenue Has

What Happened?

07:00	NASDAQ experienced a series of unexplained trading interruptions; trading suspended at 09:45.
09:03	NYSE suspended trading at 09:03. – Unexplained service outage starting at 08:28. – Securities & Exchange Commission (SEC) directed suspension of all trading at 09:22.

Yesterday

All Times PST

What Happens Now?

- SEC and CFTC close securities and commodities exchanges for two days while root-cause analysis proceeds.
- NYSE and NASDAQ execute cyber incident response plans.
  - FBI, US Secret Service, and NSA engaged.
- National Cybersecurity and Communications Integration Center (NCCIC) convenes interagency crisis action team via secure videoconference.
- Interagency meeting with National Security Council (NSC) and National Economic Council scheduled for tomorrow morning at the White House including: Depts. of Treasury, Justice, State, Homeland Security (DHS), and Defense (DoD), and the Central Intelligence Agency.

Active Players

Today

All Times PST

What Happened?

01:15	Major Internet/telecom outages affect public and private sectors from San Francisco to Sacramento. – DNS attack disables much of California state agency Internet service. – State agencies using AT&T or Integra for Internet or VOIP affected. – Attackers apparently compromised the registration of the ca.gov domain. – CA CISO fears possible massive loss of PII.
09:45	Air traffic data to Radar Approach Control at New York, Chicago, Atlanta, and Los Angeles corrupted; revert to manual operations. Major flight delays on all routes: 11,000 flights cancelled by 14:30.
15:18	An Iranian hacking collective – Cyber Fighters of Izz ad-Din al-Qassam – has claimed credit for yesterday's attacks on the financial markets.

Today

All Times PST

What Happens Now?

- California Agencies execute Continuity of Operations Plans.
- AT&T and Integra implement workarounds.
- California Information Security Office and agencies confer with MS-ISAC and Cal-CSIC on scope of incidents, current threat environment, response actions.
- Cal-CSIC Cyber Incident Response Team activated.
- US CERT focuses resources on California incidents.

Other Actions

- DoD and Intelligence Community (IC) increase intelligence collection, fusion, and analysis on al-Qassam Cyber Fighters.
- FAA Office of Information Technology (OIT) and Air Traffic Organization (ATO) respond.
- NSC holds interagency meetings.
- White House announces President will speak to nation tomorrow at 10:00.

Tomorrow

All Times PST

San Francisco Chronicle

SIMULATED

Suspecting cyber attack, FBI takes lead role in investigation, gathers computer evidence

Port of Oakland in chaos; halts operations

Officials say computerized container tracking system 'went haywire' and was shut down

The bucolic oak- and chaparral-covered ridges and valleys on the old Roddy Ranch were all set to be paved over for luxury homes, forever cutting off a wildlife corridor at the foot of Mount Diablo.

The envisioned neighborhood in Contra Costa County was going to replace habitat for threatened and endangered species with swimming pools, manicured lawns and all the Rockwellian comforts that meet the criteria of wealthy suburbanites and their requisite homeowners associations.

So it was a happy surprise for conservationists this past week when they learned that the East Bay Regional Park District was instead buying the 1,503 acres of ranchland and turning it into a regional park, forever ending the concrete

What Happened?

07:12	27 major US and Canadian national and regional banks are experiencing a DDOS attack, preventing customer access to online banking services.
09:42	Port operations interrupted in Long Beach and Oakland possibly due to hacker activity (e.g., loss/corruption of container/barcode data). Port shut down. – Operators have lost capability to monitor and control container movements and cargo storage.
Noon	California agencies continue to recover with degraded communications and alternate facilities.

Tomorrow

All Times PST

What Happens Now?

- Banks engage with FS-ISAC; apply lessons from previous DDOS events; many banks shut down wire transfers. FBI and network service providers responding.
- Port operators in Oakland and Long Beach execute crisis response plans; confer with Maritime ISAC; LB Harbor Commission and Oakland Port Commissioners meet.
- Governor briefed by CAL STAC; Cal-CSIC, FS-ISAC, Maritime ISAC integrate information.
- DHS leading major integrated response of federal agencies: FBI, National Counterterrorism Center, NSA, DoD/JCS, Depts. of Treasury, State, and Transportation.
- White House Situation Room briefing to the President at 14:00; NSC Principals meeting set for 16:00. **Big question: How are these events related?**

Other Actions

- DoD and IC increase intelligence collection, fusion, and analysis on al-Qassam Cyber Fighters.
- NSC holds interagency meetings.
- White House delay's President's address to nation until tomorrow at 10:00.

Tomorrow + 1

All Times PST

"All the News That's Fit to Print"

The New York Times

Late Edition

VOL.CXXXVII . . . No. 47,298 NEW YORK, FRIDAY FEBRUARY 19, 2016 30 CENTS

CYBER ATTACK STUNS NATION; BANKS, STOCK MARKETS, AIR TRANSPORTATION SHUT DOWN

President puts military on worldwide alert

Command & Control degraded globally

By STEVEN V. ROBERTS

A Huge Blow to the Five-Year Bull Market

Dow's Record Fall

SIMULATED

WORLDWIDE IMPACT

Full extent unknown as U.S., Allies work jointly to find cause

By LAWRENCE J. De MARIA

North Korea claims cyber attack that shut down California ports

By ERIC GELMAN

What Happened?

04:00	The switching system of the PG&E Kelso electrical substation fails; substation off line. – Initial indications are that control circuits failed simultaneously; potential SCADA system faults. – Power interruption is affecting the nearby Harvey O. Banks Pumping Plant; now operating at one-fourth of capacity.
06:20	Multiple cut fiber optic cables in Livermore and Berkeley, and Glendale, CA and Fairfax, VA affecting government networks in DC and FEMA Region IX. – CNN reports that US military command and control systems are degraded.
07:42	North Korean leader Kim Jong-Un claims that NK cyber forces hacked the port operations databases of Long Beach and Oakland causing inability to track cargo containers.

Tomorrow + 1

All Times PST

What Happens Now?

- Crisis response coordination moved from DHS to the Pentagon/National Military Command Center; Vice President, JCS, SecDef, and SecDHS briefing at 12:00.
- CalOES activates State Operations Center.
- Banks Pumping Station response (DWR and OES) coordinated at Sacramento control center through both normal and emergency communications channels.
- PG&E responding at Kelso; Electrical ISAC searches for cyber link.

BREAKING NEWS

Kim Jong-Un has just declared that inside one of the containers at the Port of Oakland is a nuclear bomb that will be detonated in 48 hours if the United States does not recognize North Korea's territorial claims to the disputed Yeonpyeong, Baengnyeong, and Daecheong Islands near the 1953 UN-imposed Northern Line Limit.

Scenario Wrap-up

Summary Points

- Many events occur in the US daily; not all are related.
- Many players are involved in crisis and emergency response.
  - Response occurs at multiple levels – mainly local.
  - But decision making requires broader scope of knowledge.
- Information sharing is a key to managing crises.
- Response plans need to be exercised and organizational structures continually managed to maintain preparedness.
- In the aftermath of an event, confusion, incorrect information, and ambiguity are common.
  - Decision making structures are challenged.
  - Time pressures need to be managed.

The Takeaway Message

- Sophisticated cyber attackers are at work.
- California state, county, and city agencies have a *fourfold* cybersecurity challenge:
  - Protecting the security of private citizen data.
  - Preserving the online availability and integrity of state services.
  - Guiding and supporting citizens and businesses in cybersecurity.
  - Responding to cyber incidents affecting California.
- All levels of government – federal, state, tribal, county, and city – must work together to protect against and respond to cyber intrusions.

Sources

- *Wall Street Journal* image: https://upload.wikimedia.org/wikipedia/en/thumb/6/69/Wall_Street_Journal_28April2008.jpg/235px-Wall_Street_Journal_28April2008.jpg.
- *Sacramento Bee* image: https://search.yahoo.com/yhs/search?p=sacramento+bee+images&ei=UTF-8&hspart=mozilla&hsimp=yhs-001.
- *San Francisco Chronicle* image: https://s.yimg.com/fz/api/res/1.2/mU4.P9hTUUtVRIi5joUM3g--/YXBwaWQ9c3JjaGRkO2g9NDAyO3E9OTU7dz02MDA-/http://scotthaefner.com/photos/images/fullsize/kap/oaklandPort04.jpg.
- *Port of Oakland* photo: https://images.search.yahoo.com/images/view;_ylt=AwrB8qFUObVWVz8As5AunIlQ;_ylu=X3oDMTIycXBramF1BHNlYwNzcgRzbGsDaW1nBG9pZAM5ZWZlOWUyNjA3NDdhODBlYjBjYzhjNzUzYzA3ZjQyYQRncG9zAzEEaXQDYmluZw--?.origin=&back=https%3A%2F%2Fimages.search.yahoo.com%2Fyhs%2Fsearch%3Fp%3DPort%2Bof%2BOakland%2BImages%26fr%3Dyhs-mozilla-001%26hsimp%3Dyhs-001%26hspart%3Dmozilla%26tab%3Dorganic%26ri%3D1&w=500&h=351&imgurl=c1.staticflickr.com%2F3%2F2689%2F4321117233_84ba6ed1f0_z.jpg%3Fzz%3D1&rurl=http%3A%2F%2Fflickr.com%2Fphotos%2Fml_kap%2F4321117233&size=153.4KB&name=Container+ship%2C+%3Cb%3EPort+of+Oakland%3C%2Fb%3E+|+Flickr+-+Photo+Sharing!&p=Port+of+Oakland+Images&oid=9efe9e260747a80eb0cc8c753c07f42a&fr2=&fr=yhs-mozilla-001&tt=Container+ship%2C+%3Cb%3EPort+of+Oakland%3C%2Fb%3E+|+Flickr+-+Photo+Sharing!&b=0&ni=84&no=1&ts=&tab=organic&sigr=11a0bc7lj&sigb=1448l6fpg&sigi=11rnq34cu&sigt=120vij3u9&sign=120vij3u9&.crumb=lubxpxz.Dfw&fr=yhs-mozilla-001&hsimp=yhs-001&hspart=mozilla.
- *New York Times* image: https://search.yahoo.com/yhs/search?p=new+york+times+stock+market+1987+cover+page+images&ei=UTF-8&hspart=mozilla&hsimp=yhs-001.

Contact Us

MARSH RISK CONSULTING

Thomas A. Fuhrman
Managing Director
Cybersecurity Consulting & Advisory Services

1050 Connecticut Avenue, NW
Washington, DC 20036
Mobile +1 202 322 3879
thomas.fuhrman@marsh.com
www.marsh.com

MARSH

ANNEX A

Reference Digest: State Cyber Resources

California Cyber Resources and Missions

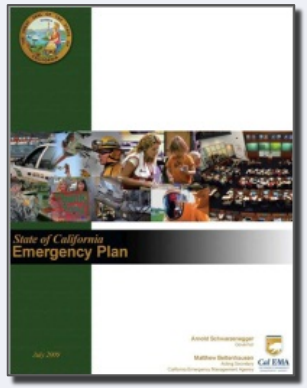
Resource	*Plan/ Strategize*	*Assess/ Prevent*	*Train/ Exercise*	*Respond*	*Coordinate*
State of California Emergency Plan	✘				
Governor's Office of Emergency Services	✘	✘	✘	✘	✘
California Information Security Office	✘	✘			
California State Threat Assessment Center (STAC)		✘			
California Military Department	✘	✘	✘	✘	✘
California Cybersecurity Integration Center (Cal-CSIC)					✘
Multi-State Information Sharing and Analysis Center (MS-ISAC)	✘	✘		✘	✘
Cybersecurity Task Force					✘
Council of Governors	✘				✘

State of California Emergency Plan

Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	Coordinate

Outlines state-level strategy to support local government efforts during a large-scale emergency, describing:

- Methods for carrying out emergency operations.
- The process for rendering mutual aid.
- Emergency services of governmental agencies.
- How resources are mobilized.
- Emergency public information.
- Continuity of government.



Governor's Office of Emergency Services

Plan/ Strategize | Assess/Prevent | Train/Exercise | Respond | Coordinate

- Responsible for the coordination of overall state agency response to disasters. Scope includes all hazards to people, property, economy, and the environment.
  - In earthquakes, floods, wildfires, drought, public health emergencies, cybersecurity attacks, agricultural and animal disasters, and threats to homeland security.
- Coordinates and supports critical emergency response activities including State Operations Center (SOC) activations.
  - Coordinates the Operational Readiness Teams; CalEOC design, development, and implementation; and Emergency Functions and external partner integration into California's emergency management system.
- **Critical Infrastructure Protection**. Protect, secure, and mitigate vulnerabilities to California's critical infrastructure assets and systems by using risk-based methodologies, security assessments, and information-sharing practices and tools with all levels of government, security managers, asset owners, and operators.
- **Telecommunications**. Coordinates emergency communications services, systems, and planning with local, state, and federal emergency operations staff, communications subject matter experts.

California Information Security Office

Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	Coordinate

- Primary state government authority in ensuring the confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information.
- Represents California to the federal, state, and local government entities, higher education, private industry, and others on security-related matters.

California State Threat Assessment Center (STAC)

	Plan/ Strategize		Assess/Prevent		Train/Exercise		Respond		Coordinate

- California's primary information fusion center; centerpiece of the state's Information Sharing Environment (ISE).
- Enables the state to maintain situation awareness over a broad range of threat domains.
- Provides strategic threat analysis to statewide leadership, policy makers, and private sector partners.
- Analysis is focused on:
  - Terrorist and extremist threats to the public, critical infrastructure, and key resources.
  - Criminal threats to the public welfare.
- Built as a direct result of the events of 9/11.
- Operated by California Highway Patrol (CHP), Governor's Office of Emergency Services (Cal OES), and California Department of Justice (Cal DOJ).

California Military Department

Plan/ Strategize | Assess/Prevent | Train/Exercise | Respond | Coordinate

- A diverse, community-based organization comprised of four pillars:
  - California Army National Guard.
  - California Air National Guard.
  - California State Military Reserve.
  - California Youth and Community Programs.
- More than 23,000 soldiers, airmen, and state military reservists.
- Operates the Cyber Network Defense program.
  - Assists the Department of Defense, federal, state, and local government partners and Critical Infrastructure providers to provide confidentiality, integrity, and availability of critical network infrastructure.
- The Cyber Network Defense Team also provides support and assistance through established partnerships with cybersecurity venders, academia, and government entities.

California Cybersecurity Integration Center (Cal-CSIC)

Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	Coordinate

- California's primary unit to lead cyber threat detection, reporting, and response.
- Formally established within OES by Governor Brown in August 2015.
- Works closely with the California State Threat Assessment System and DHS.
- Will facilitate integrated information sharing and communication with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and non-governmental organizations.
- Will establish a multi-agency Cyber Incident Response Team to serve as the state's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state.
- Includes representation from California agencies, DHS, FBI, Secret Service, Coast Guard, California Utilities Emergency Association, and others.
- Responsibilities:
  - Information sharing.
  - Warnings of cyber attack.
  - Assess risks to networks.
  - Support public and private partners in protecting their vulnerable infrastructure.
  - Develop state-wide strategy.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	**Coordinate**

Mission: Improve cybersecurity posture of state, local, tribal, territorial governments.

- Membership from all 50 states, the District of Columbia, as well as US territories, tribal governments, and local governments.
- Collaboration and information sharing among members, private sector partners, and the US Department of Homeland Security (DHS).
- Designated by DHS as the cybersecurity ISAC for State, Local, Territorial, Tribal governments.

Objectives:

- Provide two-way sharing of information and early warnings on cybersecurity threats.
- Provide a process for gathering and disseminating information on cybersecurity incidents.
- Promote awareness of the interdependencies between cyber and physical critical infrastructure as well as between and among the different sectors.
- Coordinate training and awareness.
- Ensure that all necessary parties are vested partners in this effort.

Cybersecurity Task Force

	Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	Coordinate

- Statewide public-private partnership to address the cyber threat to networks, personal privacy, and critical infrastructure.
- Established by Office of Emergency Services and the California Department of Technology.
- Comprised of key stakeholders, subject matter experts, and cybersecurity professionals from California's public sector, private industry, academia, and law enforcement.
- Advisory body to the State of California Senior Administration Officials in matters related to Cybersecurity.
- Fosters a culture of cybersecurity through education, information sharing, workforce development and economic growth.
- Advance the State's cybersecurity and position California as a national leader and preferred location for cyber business, education, and research.
- Convened by the California Homeland Security Advisor and the California Department of Technology to address cyber-related issues impacting California.

Council of Governors

Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	Coordinate
■				■

- A mechanism for governors and key federal officials to address matters pertaining to the National Guard, homeland defense, and defense support to civil authorities.
- Consists of 10 governors appointed by the President – five from each party – with two governors serving as co-chairs.
- The Council recommends:
  - The federal government should work with states to improve mechanisms for sharing threat information, expand the adoption of cybersecurity best practices and provide technical support to protect computer networks and other related critical infrastructure.
  - States should be fully integrated into national cyber incident response plans and processes must be established and tested to ensure coordination and communications between federal and state authorities during cyber incidents are effective and consistent.

ANNEX B

Reference Digest: Federal Cyber Resources

Federal Government Cyber Resources and Missions

Resource	*Plan/ Strategize*	*Assess/ Prevent*	*Train/ Exercise*	*Respond*	*Coordinate*
Department of Homeland Security	✘	✘	✘	✘	✘
Department of Defense	✘	✘	✘	✘	✘
Federal Bureau of Investigation		✘	✘	✘	✘
National Security Agency		✘	✘	✘	✘
Federal Emergency Management Agency (FEMA)				✘	✘
National Institute of Standards and Technology	*Research, standards, and guidance.*				

Note: The missions and jurisdictions of federal agencies in the identified functional areas are prescribed by law. Operationalizing these functions may require authorities invoked by appropriate presidential declarations.

Department of Homeland Security (DHS)

Plan/ Strategize | Assess/Prevent | Train/Exercise | Respond | Coordinate

Selected DHS Cyber Resources

- Operates the National Cybersecurity and Communications Integration Center (NCCIC).
  - 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement.
  - Shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations.
- US Computer Emergency Readiness Team (US-CERT) applies advanced network and digital media analysis of malicious activity targeting our nation's networks.
- Develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors.

Department of Defense (DoD)

Plan/ Strategize | Assess/Prevent | Train/Exercise | Respond | Coordinate

Selected DoD Cyber Resources

- **Cyber Threat Intelligence Integration Center**
  - Created by the President in February 2015 to fill inter-agency information gaps regarding cyber threats.
  - Will analyze and integrate information that is already collected under existing authorities.
  - Enable centers that already perform cyber functions to be more effective.
  - Private sector assistance: when companies share information about a cyber attack, the government can provide assistance by:
    - Providing information about the threat.
    - Coordinating a quick and unified response from government experts, including those at DHS and FBI.
    - Determining who the actors are.
    - Applying government tools and resources to disrupt threats.
- **Exercises**. National Guard annual “Cyber Guard” exercise.
  - Involves government, academia, industry, and international partners in large-scale cyber threat drills.

Federal Bureau of Investigation (FBI)

Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	Coordinate

Selected FBI Cyber Resources

- Cyber Division
  - Investigation of cyber crime cases by f terrorist organizations, foreign government-sponsored intelligence operations, or criminal activity.
  - Forms and maintains public/private alliances to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities.
  - Maintains awareness of emerging technology.
- National Cyber Investigative Joint Task Force (NCIJTF)
  - In partnership with the DoD Cyber Crime Center.
  - Mission includes helping protect critical infrastructures, industry, and international partners.
- Cyber Task Forces (CTF)
  - Presence in all 56 national field offices.
  - Promotes effective collaboration and deconfliction of efforts at local and national levels.
- Cyber Action Team (CAT)
  - Rapid deployment of cyber experts – can be on-scene almost anywhere in the world within 48 hours to provide investigative support.
- National Cyber-Forensics & Training Alliance (NCFTA)
  - Law enforcement, private industry, and academia build and share resources, strategic information, and threat intelligence to stop emerging cyber threats and mitigate existing ones.

National Security Agency (NSA)

Plan/ Strategize | Assess/Prevent | Train/Exercise | Respond | Coordinate

Selected NSA Cyber Resources

- Information Assurance Directorate (IAD)
  - Protects and defends National Security Information and Information Systems (systems that handle classified information and other critical military or intelligence information).
  - Widely acknowledged for leading innovative security solutions.
  - Partners extensively with government, industry, and academia to protect and defend information systems and national critical infrastructure.
- National Security Cyber Assistance Program (NSCAP)
  - Leverages the expertise of the cyber industry. Objectives:
    - Develop a list of “accredited” cyber service providers from which the National Security System (NSS) community can draw upon for timely cyber assistance.
    - Promote public-private collaboration.
    - Leverage industry expertise to protect national interests.
    - Address this growing concern across the government.
- National Centers of Academic Excellence in Cyber Defense (CAE-CD) program.
- Jointly sponsor with DHS to promote higher education and research in cyber defense and produce professionals with cyber defense expertise.

Federal Emergency Management Agency (FEMA)

Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	Coordinate
■				■

- FEMA's mission is to prepare for, protect against, respond to, recover from, and mitigate all hazards.
- FEMA Region 9, headquartered in Oakland, California, is one of ten Regional Offices.
- On call 24/7, FEMA people are experts in the various fields of emergency management.
- FEMA Region 9 supports the development of a regional, all-hazards, risk-based emergency management system of preparedness, prevention, protection, response, recovery, and mitigation.

- Nurtures close working relationships among federal agencies, state, tribal nations, localities, business and industry, and state and local volunteer organizations and faith-based groups.
- Cal-OES (Office of Emergency Services) interfaces and works closely with FEMA through all phases of emergency management: mitigation, preparedness, response, and recovery.

National Institute of Standards and Technology (NIST)

Plan/ Strategize	Assess/Prevent	Train/Exercise	Respond	Coordinate

NIST is a non-regulatory federal agency with the mission to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology.

Selected NIST Cyber Resources

- Computer Security Division (CSD)
  - Responsible for developing standards, guidelines, tests, and metrics for protection of non-national security federal information systems.
  - While developed for federal agency use, CSD products are accepted globally.
  - Conducts the research, development, and outreach to provide standards and guidelines, mechanisms, tools, metrics and practices to protect US information and information systems.
  - CSD comprises the following groups:
    - Cryptographic Technology.
    - Secure Systems and Applications.
    - Security Components and Mechanisms.
    - Security Outreach and Integration.
    - Security Testing, Validation, and Measurement.
- Applied Cybersecurity Division (ACD) comprises the following groups:
    - Cryptographic Technology.
    - Secure Systems and Applications.
    - Security Components and Mechanisms.
    - Security Outreach and Integration.
    - Security Testing, Validation, and Measurement.

MARSH RISK CONSULTING

MA16-13874