Incident Response Training

North Central Texas Council of Governments

Incident Response Training

Part 1 –

Incident Response – The Big Picture

Agenda ❯

1. Incident, Incident Response and Life Cycle
2. NIMS Overview and Incident Command System (ICS)
3. Incident Response, ICS and Escalations
4. Incident Response Preparation and Administration
5. IR Roles and Responsibilities
6. Testing and Training

Agenda

1. **Incident, Incident Response and Life Cycle**
2. NIMS Overview and Incident Command System (ICS)
3. Incident Response, ICS and Escalations
4. Incident Response Preparation and Administration
5. IR Roles and Responsibilities
6. Testing and Training

What is an Incident?

An incident is . . .

. . . an occurrence, caused by either human or natural phenomena, that requires response actions to prevent or minimize loss of life, or damage to property and/or the environment.

A Cyber Security incident is . . .

. . . an adverse event (or threat of an adverse event) in a computer system in the following general categories:

- Compromise of Confidentiality
- Compromise of Integrity
- Denial of Resources
- Intrusions
- Misuse
- Damage
- Hoaxes

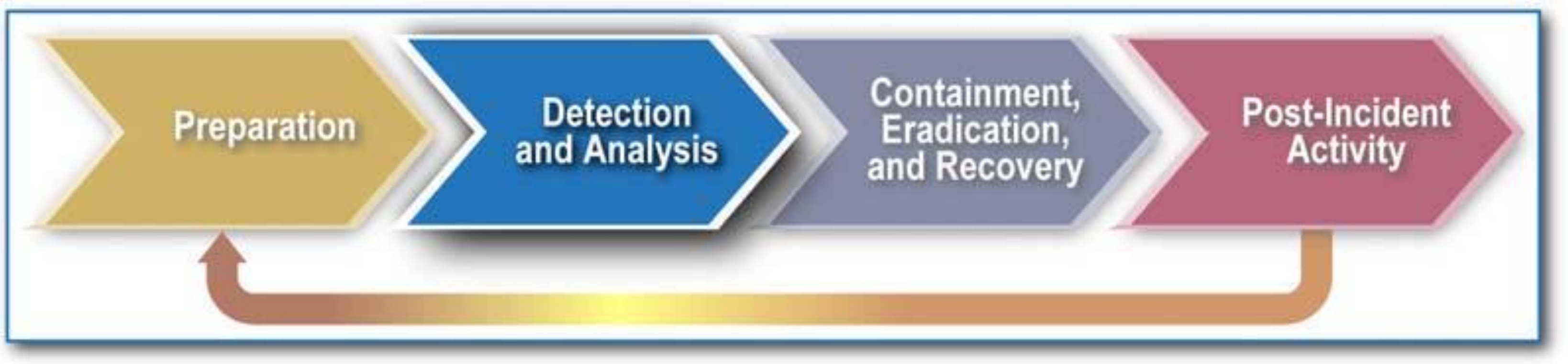
Preparation matters: Hint - The key word in an incident plan is not 'incident'; preparation is everything.

Incident Management Life Cycle

Incident response (IR) is the effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.

Plan, Prepare, Manage, Mitigate and Remediate

- **Plan** – Have a plan and test it
- **Prepare** – Create a CIRT and practice scenarios
- **Manage** – Have a program for managing an incident
- **Mitigate** – Plans of Action to mitigate common scenarios
- **Remediate** – Action plan for addressing gaps and issues



Agenda

1. Incident, Incident Response and Life Cycle
2. **NIMS Overview and Incident Command System (ICS)**
3. Incident Response, ICS and Escalations
4. Incident Response Preparation and Administration
5. IR Roles and Responsibilities
6. Testing and Training

STEALTH ISS GROUP

NORTH CENTRAL TEXAS COUNCIL OF GOVERNMENTS

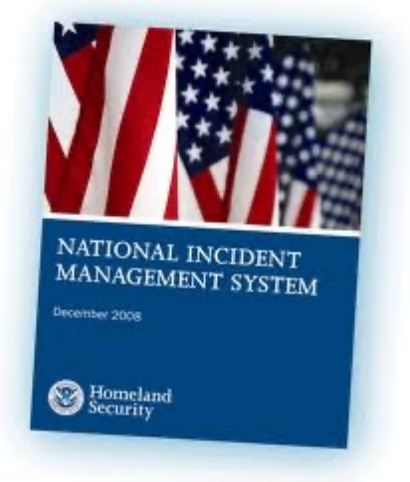
National Incident Management System - NIMS Overview

- **What ? . . .** NIMS provides a consistent nationwide template . . .

- **Who? . . .** to enable Federal, State, tribal, and local governments, the private sector, and nongovernmental organizations to work together . . .

- **How? . . .** to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents regardless of cause, size, location, or complexity . . .

- **Why? . . .** in order to reduce the loss of life and property, and harm to the environment.



NIMS: What it is and What it is not

NIMS Is…

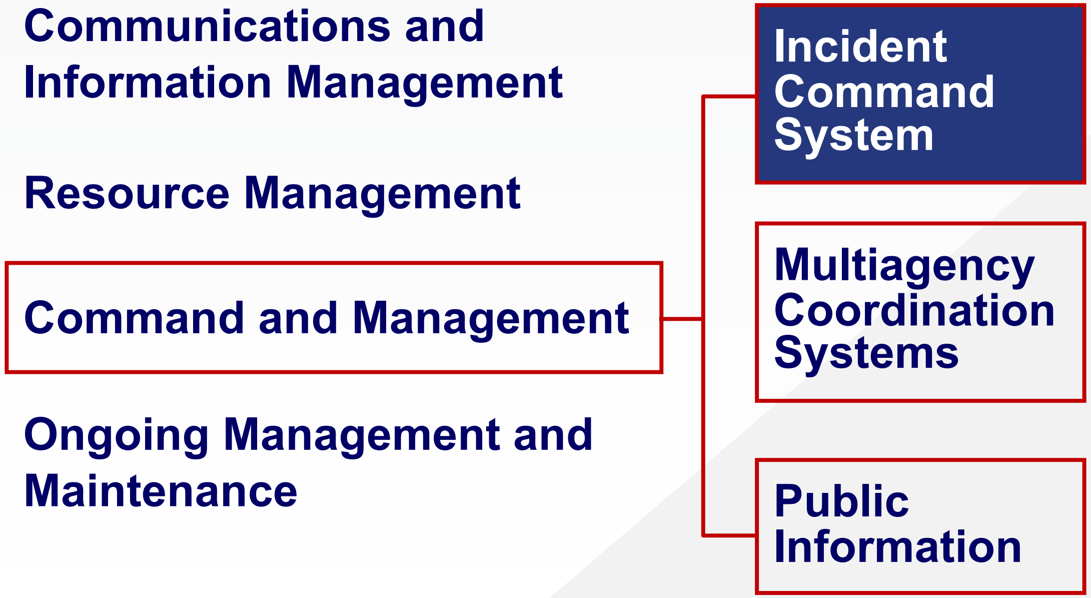
- Comprehensive, nationwide, systematic approach to incident management
- Set of preparedness concepts and principles for all hazards
- Essential principles for a common operating picture and interoperability of communications and information management
- Standardized resource management procedures for coordination among different jurisdictions/ organizations
- Scalable and applicable for all incidents

NIMS Is Not…

- A response plan
- A communication plan
- Something that is used only during large incidents
- Only applicable to certain emergency responders
- Only the Incident Command System or an organizational chart
- A static system

NIMS Components

Preparedness



Communications and Information Management

Resource Management

Command and Management

- Incident Command System
- Multiagency Coordination Systems
- Public Information

Ongoing Management and Maintenance

Incident Command System (ICS) and its usage

What is ICS:

- Is a standardized, on-scene, all-hazards incident management concept.
- Enables a coordinated response among various jurisdictions and agencies.
- Establishes common processes for planning and management of resources.
- Allows for integration within a common organizational structure.

When Is ICS Used?

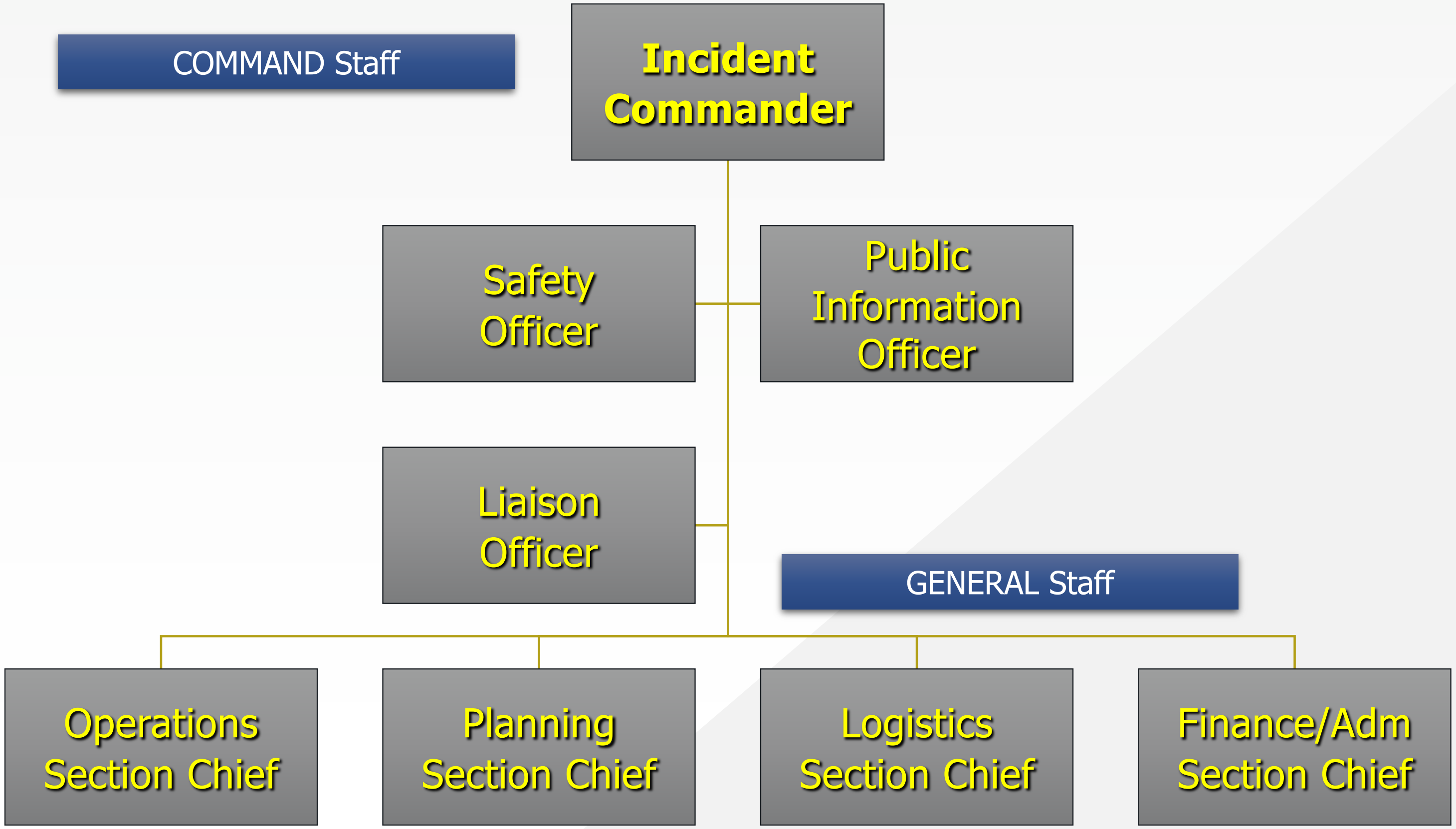
ICS can be used to manage:

- Natural hazards
- Technological hazards
- Human-caused hazards
- Planned events

Without ICS, incident responses typically:

- Lack accountability
- Have poor communications
- Use unsystematic planning processes
- Are unable to efficiently integrate responders

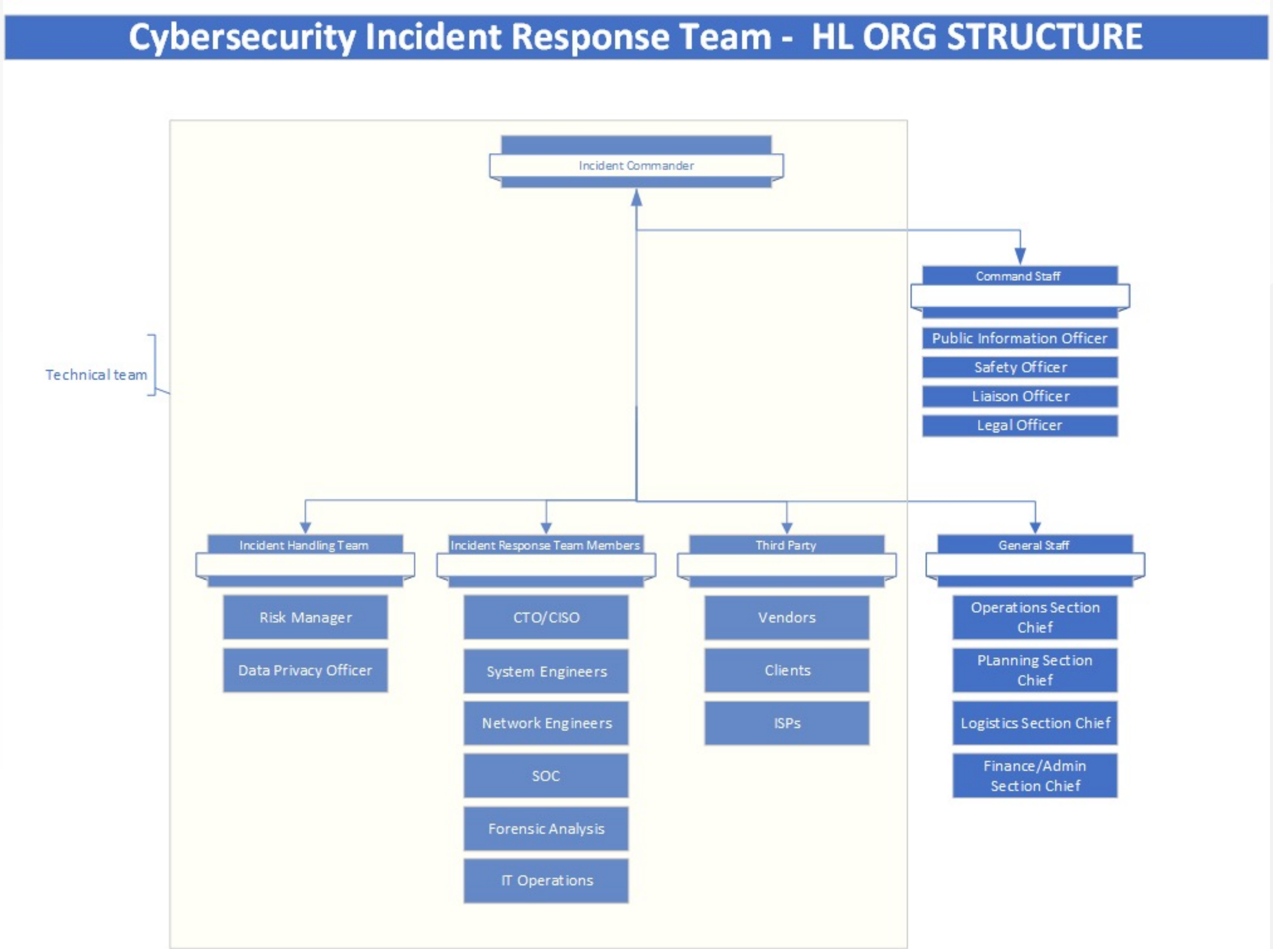
ICS Command and General Staff



Agenda

1. Incident, Incident Response and Life Cycle
2. NIMS Overview and Incident Command System (ICS)
3. **Incident Response, ICS and Escalations**
4. Incident Response Preparation and Administration
5. IR Roles and Responsibilities
6. Testing and Training

Incident Response and ICS Command



Cybersecurity Incident Response Team - HL ORG STRUCTURE

Incident Commander

Technical team

Command Staff

- Public Information Officer
- Safety Officer
- Liaison Officer
- Legal Officer

Incident Handling Team

- Risk Manager
- Data Privacy Officer

Incident Response Team Members

- CTO/CISO
- System Engineers
- Network Engineers
- SOC
- Forensic Analysis
- IT Operations

Third Party

- Vendors
- Clients
- ISPs

General Staff

- Operations Section Chief
- PLanning Section Chief
- Logistics Section Chief
- Finance/Admin Section Chief

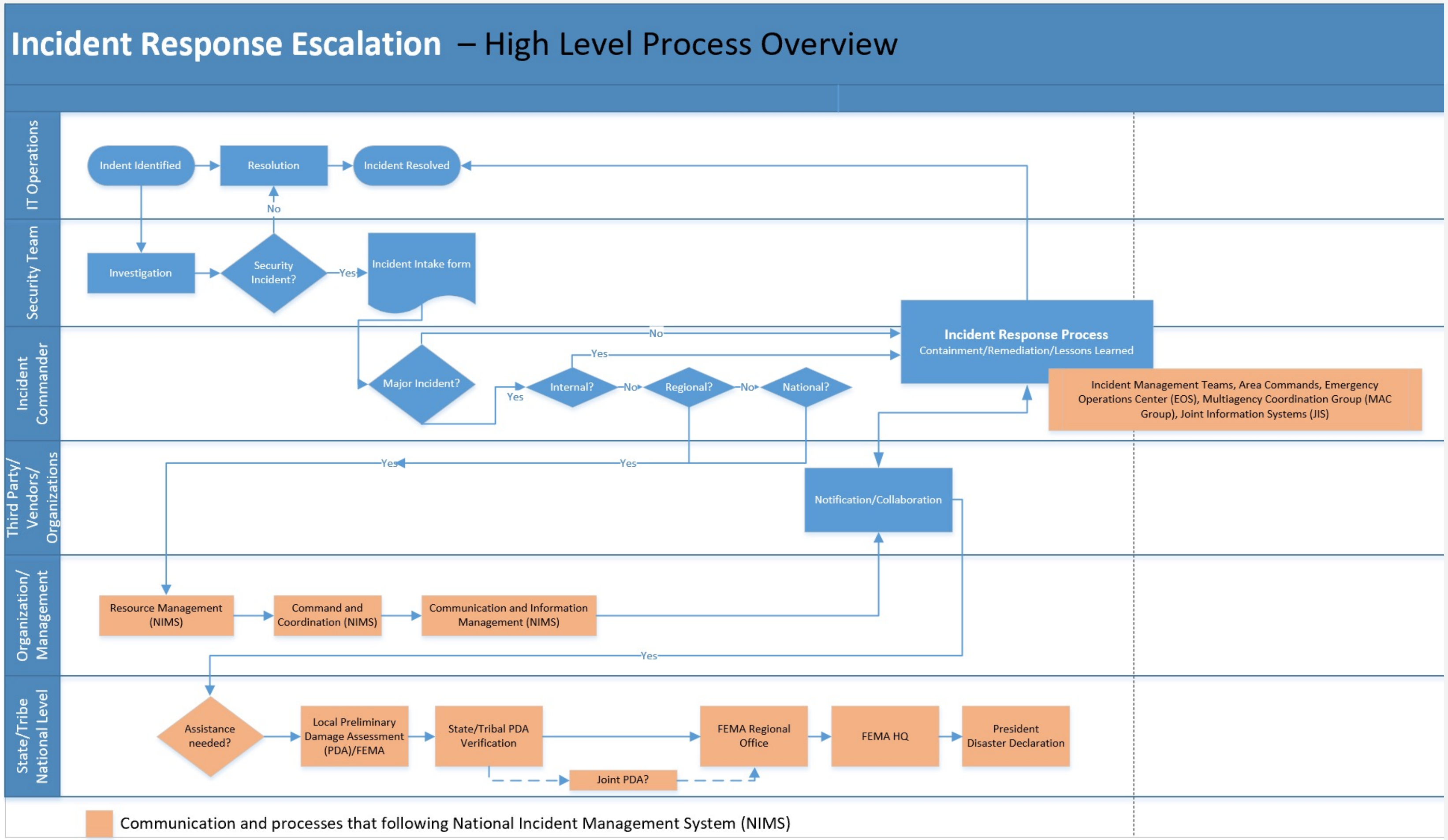
www.stealth-iss.com

STEALTH ISS GROUP

NORTH CENTRAL TEXAS COUNCIL OF GOVERNMENTS

Incident Response Escalations

www.stealth-iss.com



Incident Response Escalation – High Level Process Overview

IT Operations

Indent Identified → Resolution → Incident Resolved

Security Team

Investigation → Security Incident? — Yes → Incident Intake form

Security Incident? — No → Resolution

Incident Commander

Major Incident? — No → Incident Response Process

Major Incident? — Yes → Internal?

Internal? — Yes → Incident Response Process

Internal? — No → Regional? — No → National?

Incident Response Process
Containment/Remediation/Lessons Learned

Incident Management Teams, Area Commands, Emergency Operations Center (EOS), Multiagency Coordination Group (MAC Group), Joint Information Systems (JIS)

Third Party/ Vendors/ Organizations

Regional? — Yes, National? — Yes → Resource Management (NIMS)

Notification/Collaboration

Organization/ Management

Resource Management (NIMS) → Command and Coordination (NIMS) → Communication and Information Management (NIMS) → Notification/Collaboration

Notification/Collaboration — Yes → Assistance needed?

State/Tribe National Level

Assistance needed? → Local Preliminary Damage Assessment (PDA)/FEMA → State/Tribal PDA Verification → FEMA Regional Office → FEMA HQ → President Disaster Declaration

State/Tribal PDA Verification - - → Joint PDA? - - → FEMA Regional Office

🟧 Communication and processes that following National Incident Management System (NIMS)

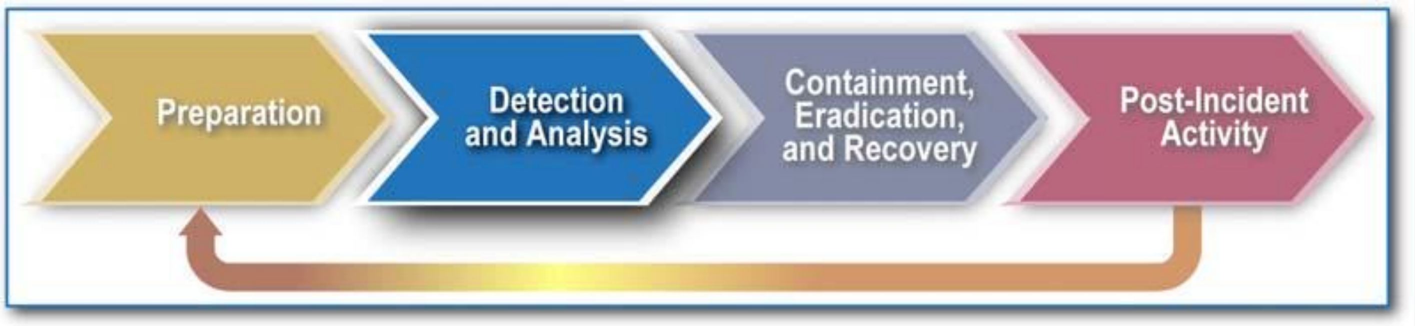
Agenda

1. Incident, Incident Response and Life Cycle
2. NIMS Overview and Incident Command System (ICS)
3. Incident Response, ICS and Escalations
4. **Incident Response Preparation and Administration**
5. IR Roles and Responsibilities
6. Testing and Training

Incident Response Preparation

Effective incident management requires preparation which includes:

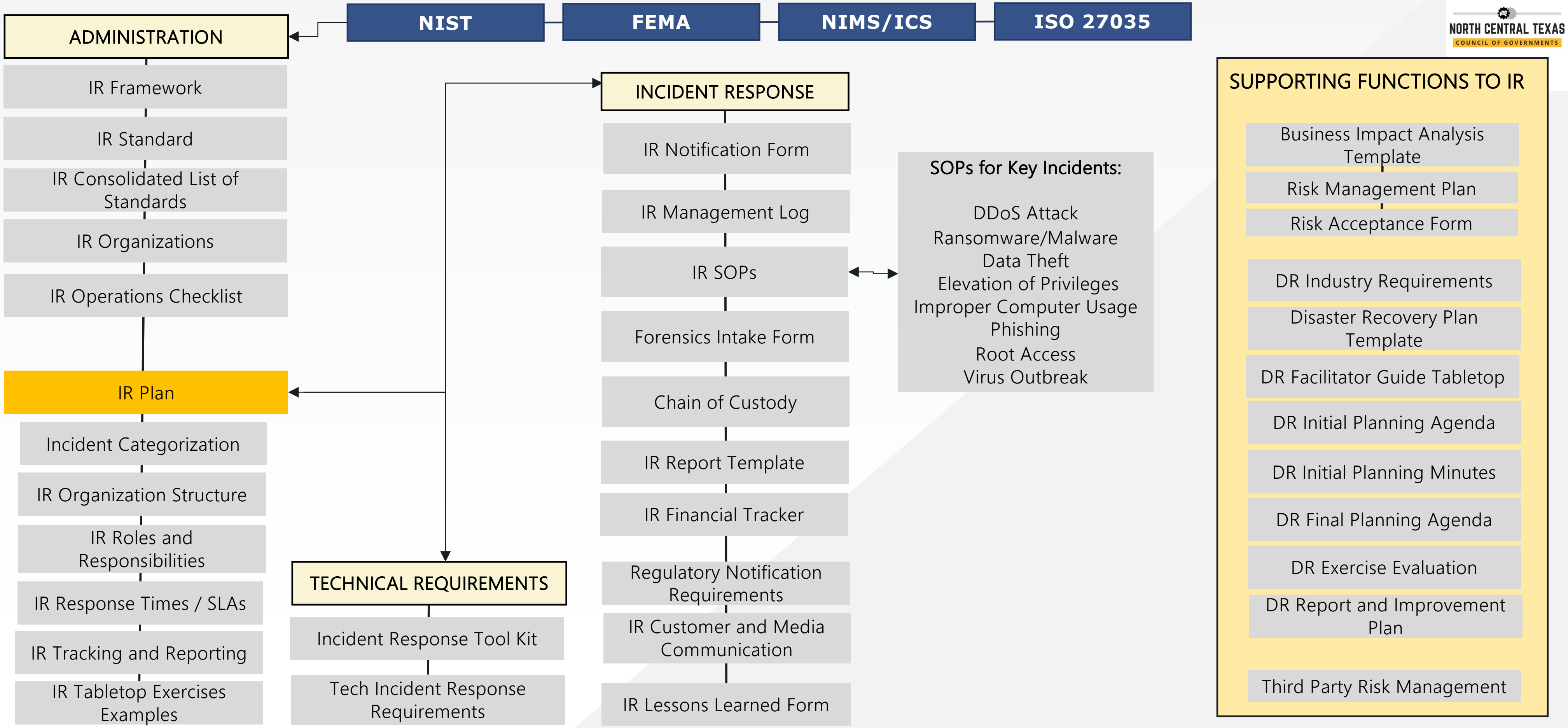
- Planning, training, and exercises
- Personnel qualification and certification standards
- Equipment acquisition and certification standards
- Publication management processes and activities
- Mutual Aid Agreements/Emergency Management Assistance Compacts



NIMS Note:

- Preparedness is the responsibility of individual jurisdictions
- NIMS provides tools to help ensure and enhance preparedness

IR Aligned with Standards



NIST

FEMA

NIMS/ICS

ISO 27035

ADMINISTRATION

- IR Framework
- IR Standard
- IR Consolidated List of Standards
- IR Organizations
- IR Operations Checklist

IR Plan

- Incident Categorization
- IR Organization Structure
- IR Roles and Responsibilities
- IR Response Times / SLAs
- IR Tracking and Reporting
- IR Tabletop Exercises Examples

TECHNICAL REQUIREMENTS

- Incident Response Tool Kit
- Tech Incident Response Requirements

INCIDENT RESPONSE

- IR Notification Form
- IR Management Log
- IR SOPs
- Forensics Intake Form
- Chain of Custody
- IR Report Template
- IR Financial Tracker
- Regulatory Notification Requirements
- IR Customer and Media Communication
- IR Lessons Learned Form

SOPs for Key Incidents:

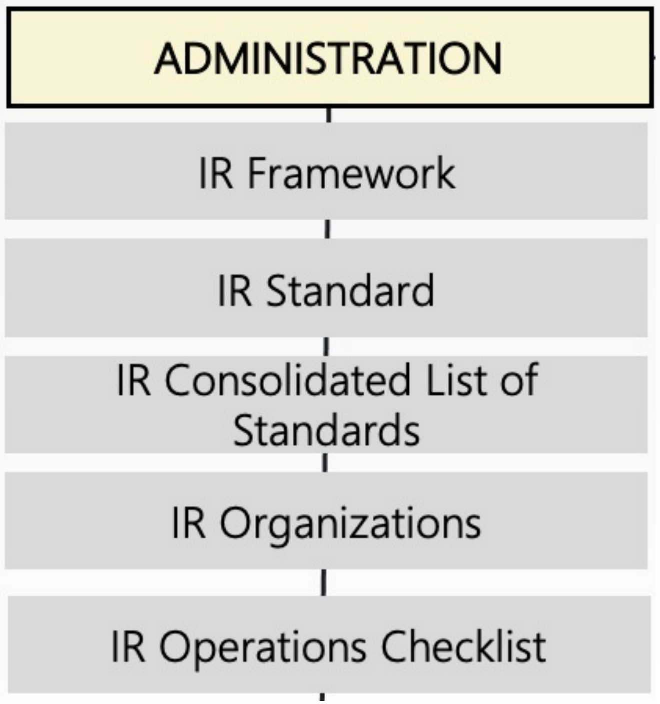
DDoS Attack
Ransomware/Malware
Data Theft
Elevation of Privileges
Improper Computer Usage
Phishing
Root Access
Virus Outbreak

SUPPORTING FUNCTIONS TO IR

- Business Impact Analysis Template
- Risk Management Plan
- Risk Acceptance Form
- DR Industry Requirements
- Disaster Recovery Plan Template
- DR Facilitator Guide Tabletop
- DR Initial Planning Agenda
- DR Initial Planning Minutes
- DR Final Planning Agenda
- DR Exercise Evaluation
- DR Report and Improvement Plan
- Third Party Risk Management

www.stealth-iss.com

Incident Response Administration



Microsoft Word Document

IR Framework

- Importance of Incident Response
- Incident Response Life Cycle
- Coordination and Information Sharing (internal and external)

IR Standard

- Aids organizations/units/locations to create IR Plans
  - Notifications
  - Assessments
  - Incident Management

IR Consolidated List of Standards

- Official websites related to IR standards, best practices and guidelines

IR Organizations

- List of various IR organizations that support or provide guidance for IR

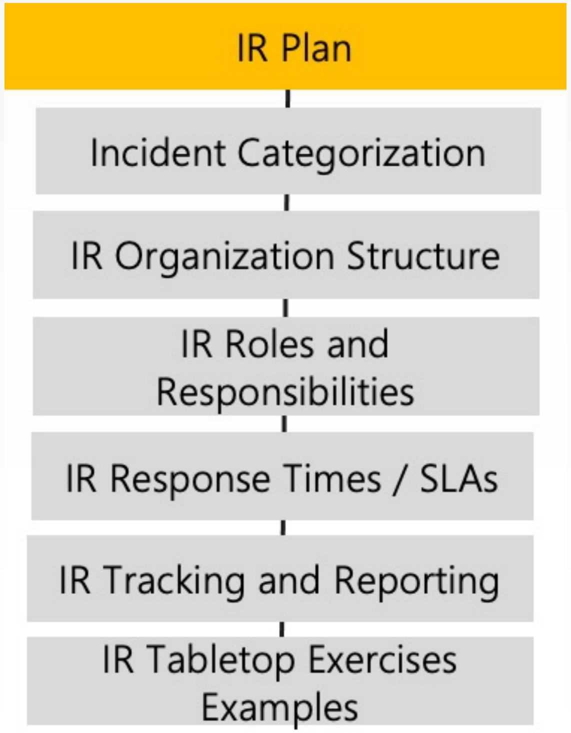
IR Organization Structure

- Positions and structure within an IR Team

IR Operations Check list

- Checklist to validate key areas of IR are addressed and in place

The Incident Response Plan



IR Plan

Incident Categorization

IR Organization Structure

IR Roles and Responsibilities

IR Response Times / SLAs

IR Tracking and Reporting

IR Tabletop Exercises Examples

An incident response plan:

- Is the most important document in Incident Response
- Defines the mission
- Outlines procedures, steps, and responsibilities
- Defines the approach to incident response and activities required in each phase of incident response
- Assigns roles and responsibilities for completing
- Maintains a contact and escalation list (internal and external)

Microsoft Word Document

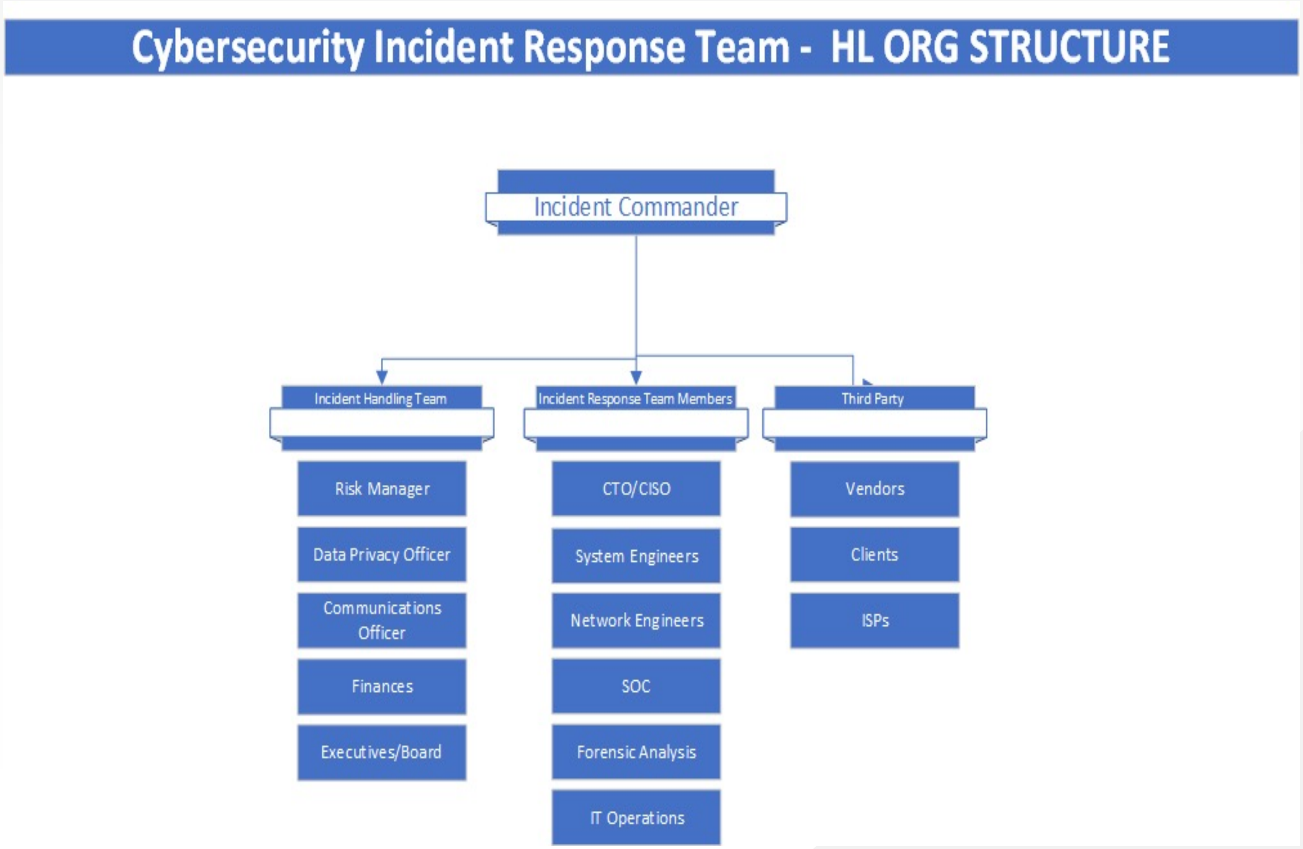
May include several documents:

- Organization, Roles and Responsibilities
- IR Table-Top Exercises
- Incident Categorization
- IR Repones Times and SLAs
- Contact lists

Agenda

1. Incident, Incident Response and Life Cycle
2. NIMS Overview and Incident Command System (ICS)
3. Incident Response, ICS and Escalations
4. Incident Response Preparation and Administration
5. **IR Roles and Responsibilities**
6. Testing and Training

Key Components: Resources



Cybersecurity Incident Response Team - HL ORG STRUCTURE

Incident Commander

- Incident Handling Team
  - Risk Manager
  - Data Privacy Officer
  - Communications Officer
  - Finances
  - Executives/Board
- Incident Response Team Members
  - CTO/CISO
  - System Engineers
  - Network Engineers
  - SOC
  - Forensic Analysis
  - IT Operations
- Third Party
  - Vendors
  - Clients
  - ISPs

- Cross Functional Team
- Organized and Coordinated
- Various Skills
- Usually responds only to major incidents
  - minor incidents are part of normal operations

Key Components: Roles and Responsibilities

Microsoft Word Document

Incident Commander

- Responsible for declaring a cyber security incident and managing team response activities
- Oversees and prioritizes actions
- Aligns and collaborates with other agencies/teams

Chief Security Information/Technology Officer (CISO/CIO/CTO)

- Coordinate response activities with auxiliary departments and external resources
- Review the Plan to ensure that it meets objectives

Cybersecurity Incident Response Team (CIRT)

- Assist in incident response e.g., review logs, analyze network traffic
- Monitor business applications
- Collect pertinent information

Incident Handling Team

- Collecting and recording incident cost
- Overseeing the maintenance of accurate, complete, up-to-date incident files
- Maintaining Incident Log and documentation
- Responsible to communicate with public and clients
- Responsible for recording key information about the incident and its response effort
- Providing context and updates to the incident team, notifying additional subject matter experts

www.stealth-iss.com

STEALTH ISS GROUP

NORTH CENTRAL TEXAS COUNCIL OF GOVERNMENTS

Agenda

1. Incident, Incident Response and Life Cycle
2. NIMS Overview and Incident Command System (ICS)
3. Incident Response, ICS and Escalations
4. Incident Response Preparation and Administration
5. IR Roles and Responsibilities
6. **Testing and Training**

STEALTH
ISS GROUP

NORTH CENTRAL TEXAS
COUNCIL OF GOVERNMENTS

Microsoft Word Document

Key Components: Testing and Training

Tabletop Exercise – What?

- Effective way to evaluate your incident response plans through practice using example incidents/scenarios
- Choose (most relevant) and address various scenarios
- Test validate processes to be used following and emergency event
- IR Team familiarity and advance collaboration - Incident Commander (IC), Cybersecurity Incident Response Team (CIRT), Incident Handling Team (IHT), Human Resources function, and Business Continuity Members

www.stealth-iss.com

Key Components: Testing and Training

Tabletop Exercise – Why?

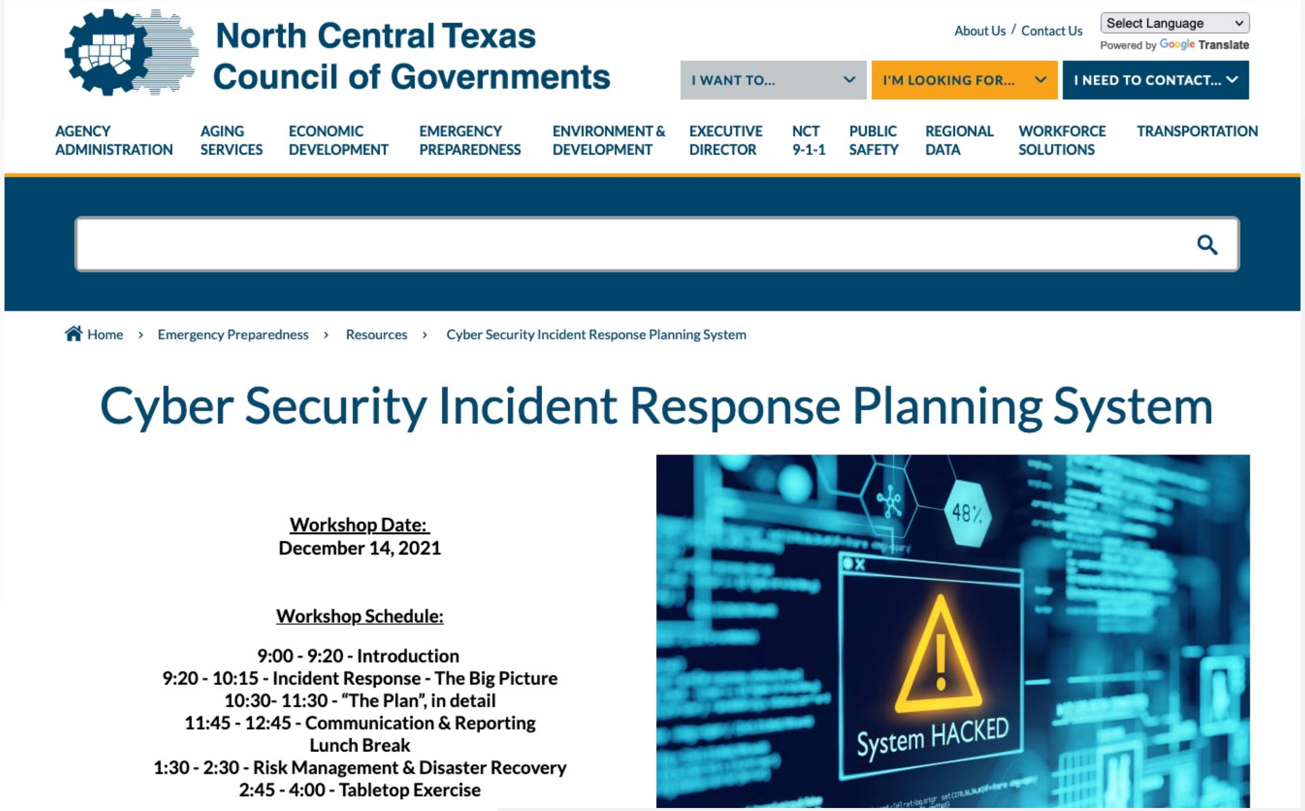
Microsoft Word Document

Reduce time to restore business operations in the event of a breach

- Help your people understand their roles and responsibilities
- Develop a better understanding of breaches and how to deal with, even prevent them
- Cost-effective way of ramping up your security defenses
- Assess and promote communication and collaboration within teams and departments, identify gaps
- List out the strengths and weaknesses of the IR processes, improve the processes
- Identify any training gaps
- Potentially Identify loopholes or defects in the Plan
- Regulatory requirement: mandatory for critical national infrastructure and banking

Questions?

Where to find documents and information?



Cyber Security Incident Response Planning System

Workshop Date:
December 14, 2021

Workshop Schedule:

9:00 - 9:20 - Introduction
9:20 - 10:15 - Incident Response - The Big Picture
10:30- 11:30 - "The Plan", in detail
11:45 - 12:45 - Communication & Reporting
Lunch Break
1:30 - 2:30 - Risk Management & Disaster Recovery
2:45 - 4:00 - Tabletop Exercise

https://nctcog.org/ep/resources/cyber-security-incident-response-planning-system

www.stealth-iss.com

THANK YOU

www.stealth-iss.com

HQ – ARLINGTON, VIRGINIA

4601 North Fairfax Drive, Suite 1200
Arlington, VA 22203

OFFICE LOCATIONS

Las Vegas, Nevada

London, England

Dubai, United Arab Emirates

Bratislava, Slovakia

Stealth-ISS Group® Inc. | www.stealth-iss.com | bizdev@stealth-iss.com