The Federal Approach to Special Events

InfraGard Jacksonville

CISA
CYBER+INFRASTRUCTURE

PSA Kirby Wedekind
June 29, 2020

Agenda

- The Federal approach to Special Events
  - National Special Security Events (NSSE)
  - Special Event Assessment Ratings (SEAR)
- Critical Infrastructure
- Planning for the Republican National Convention (RNC) in Jacksonville
  - Topics of Interest
  - Mitigation

National Special Security Events

National Special Security Event (NSSE) is an event of national significance deemed to be a potential target for terrorism or other criminal activity

Presidential Decision Directive 62 (1998) – established the framework for apprehension, prosecution, transportation security, enhanced emergency response, enhanced cybersecurity

Public Law 106-544 (2000) – authorized USSS to plan, coordinate and implement security operations

National Special Security Events

DHS Secretary holds the authority for designating events as NSSE

- Attendance by U.S. officials/foreign dignitaries
- Size of event
- Significance of event

Typical events

- Inauguration
- United Nations General Assembly (UNGA)
- National Conventions (RNC/DNC)
- State of the Union (SOTU)

National Special Security Events

Executive Steering Committee (ESC) is lead element

Unified Command Model

Federal: USSS, FEMA, FBI, HHS

State: FDLE, FDEM, FDOH

Local: City of Jacksonville, JFRD, JFRD EPD, JSO

National Special Security Events

Executive Steering Committee establishes **Subcommittees (20+)** execute the detailed planning for the event:

- Venues
- Transportation
- Tactical
- Credentialing
- Consequence Management
- **Critical Infrastructure (CI)**

Special Event Assessment Ratings

- Liaise with federal, state, and local officials
- Serve as an advisor to the Unified Coordination Group and/or incident commanders
- Resolve any federal interagency conflicts that may arise
- Consult with state and local authorities on their event security and response plans
- Ensure appropriate and coordinated federal support is occurring in response to federal-to-federal, state, and local requests for assistance
- Maintain situational awareness of the event throughout the planning and execution phases
- Provide periodic updates to DHS senior leadership as needed throughout the planning process

SEAR Levels

Level 1	• Significant national and/or international importance • May require extensive federal interagency support	• Super Bowl • Tournament of Roses Parade/Rose Bowl
Level 2	• Significant events with national and/or international importance • May require some national level federal support	• Times Square New Year's Eve • Indianapolis 500 • Boston Marathon
Level 3	• Events of national and/or international importance • Requires only limited federal support	• Daytona 500 • U.S. Open Tennis Tournament • Masters Golf Tournament
Level 4	• Limited national importance • Handled at the state/local level	• Clark County Fair and Rodeo • Orange Bowl • Calle Ocho Festival
Level 5	• Events may be nationally recognized but generally have only state/local importance • Normally handled at the local level	• Ohio Renaissance Festival • Golden Globes • U.S. Team Roping Championships

Critical Infrastructure Subcommittee

Monitor and safeguard critical infrastructure systems—both cyber and physical—that are essential to the security plan for the RNC

- Identify CI elements and conduct risk assessments
- Introspect / Self-Help
- Leverage partners for their expertise
- Meet to discuss plans and conduct assessments
- Develop incident response plans
- Plan Cyber Network Monitoring
- Indicators of Compromise (IOCs)
- Baseline normal operations/look for anomalies

Incident Response

- Cyber Incident Response (PPD-41)
  - Threat – FBI Cyber Action Team (CAT)
  - Asset – DHS Hunt and Incident Response Team (HIRT)
  - Other supporting – National Guard, HSI

- What about private sector incident responders?

Protected Critical Infrastructure Information

- Protected Critical Infrastructure Information (PCII)
  - Protects information shared by partners with government
    - Freedom of Information Act (FOIA) or state equivalent
    - Prohibited from using for regulatory action
- Access requires **training** and **need-to-know**
- Submitted to government via portal
  - https://pciims.dhs.gov

Homeland Security Information Network

- Email HSIN@hq.dhs.gov and provide the following information:
  - Name:
  - Job Title and organization:
  - Government or business email address:
  - Contact info:
  - Justification for requiring HSIN access:
  - Mission Area of Interest: Critical Infrastructure, Emergency Services
- Vulnerability_Info@cisa.dhs.gov
- Kirby.Wedekind@hq.dhs.gov

Topics of Interest

- Ransomware
  - Atlanta, Baltimore, Cities in Florida
  - Incidences increasing (willingness to pay)
- Iranian Activity
  - Phishing, DoS/DDoS, etc.
  - Incidences increasing (retaliation)

APT Defense

- Employee education/testing
- Backups (full and incremental, off-line)
- Patch management
- IR/DR plans
- Insurance
- Staffing/resources
- Exercises

Next Steps

1. Enroll in CISA's Vulnerability Scanning service
2. Sign up for HSIN
3. Sign up for NCAS Alerts
4. Engage within your organization
5. Engage with external partners

CISA
CYBER+INFRASTRUCTURE

For more information:

cisa.gov

Questions?

Email: Kirby.Wedekind@hq.dhs.gov
Phone: 202 868 1361

CISA

CYBER+INFRASTRUCTURE