DoIT Incident Response
Tabletop Exercise
February 17, 2012
DoIT Incident Response (I/R)

• Introduction
  – DoIT responds to the following:
    • Support of EOC and WebEOC during activation of any kind of state emergency
    • IT outage resolution, with various root causes
    • Security incident response
  – Responses involve varying leadership and staff involvement but have commonality of process
  – DoIT is part of incident response; agency involvement in preparation and response activities is crucial
DoIT Incident Response (I/R)

• Overview
  – Test the clarity and efficacy of I/R plans and roles
  – Effective I/R reduces incident impact and duration
  – Designed using Homeland Security Exercise and Evaluation Program (HSEEP) guidelines and with URS input
  – Discussion-based tabletop exercise conducted on Feb 8th

• Attendees & Roles
  – CISO - Tabletop designer and facilitator
  – DoIT Security Response Team (SRT) - senior management, work unit managers and technical leads split into two breakout groups
  – URS - Facilitation of breakout groups and exercise support
  – Col Routhier - Observer with objective and valued input
DoIT Incident Response (I/R)

• Scope:
  – Major operational outages
  – Security incidents with broad impact
  – Cyber-caused IT interruptions with broad impact
  – Five scenarios: people, hardware, config, cyber and event prep
  – Injects used to add to complexity and severity to scenario

• Objectives - determine if:
  – Plans, policies and procedures are accurate and complete
  – Escalation and engagement triggers are defined
  – Response leadership is assumed based on situation type
  – SRT membership is appropriate and complete
  – Identify improvements to enhance overall response capabilities
DoIT Incident Response (I/R)

• Key Results
  – Commonalities in all situation types - people, operational, cyber
  – Incident Command System (ICS) and National Incident Management System (NIMS) framework in use by HSEM crucial
  – Mixed composition teams require foundation knowledge
  – Formalize procedures with trigger and escalation points
  – Need involvement of IT Leaders as agency liaisons
  – Identify critical agency applications to prioritize efforts
  – Develop statewide prioritization for multi-agency events

• Next Steps:
  – Review participant feedback responses
  – Develop After Action Report (AAR) & Improvement Plan (IP) Matrix
  – IP tasks to be addressed by SRT members and others
DoIT Incident Response (I/R)

- **Future Exercises**
  - Broaden participation and engagement:
    - Cybersecurity Advisory Council (CAC) – Agency ISOs
    - Agencies not represented on the CAC
    - Select local government entities
    - Major NH providers and vendors such as FairPoint and Cisco
  - DHS Grant Application submitted for:
    - Two year program using iterative approach: *train, test, adjust*
    - Workshops to gain familiarity with DoIT and agency I/R plans
    - Training recommendations to build baseline knowledge
    - Tabletop - to identify strengths and improvements
    - Functional exercise - operations-based simulated response
Questions
Department of Safety
State Police
eTicketing Project

Increased Safety Using Technology
E-Ticket Objectives

- Reduced time for stops increasing public and trooper safety
- Reduce time for filing of infraction data
- Increased visibility to risky drivers
Project Teams

DOIT
• Rick Sheldon, DOS IT Leader
• Brian Lumbert, Project Mgr
• Shawn Mills, Lead Programmer
• Claire Janelle
• Marc Whitney
• Deepak Pant
• Jitin Sood
• J. Yeske

DMV
• Suzanne Roy

State Police
• Lt Jerry Maslan – SP Lead
• Lt Bill Haynes – Troop G
• Sgt John Begin
• T1C Katie Grealy
• TPR Brian Parker
• TPR Shawn Magoon

COURTS
• Paula Hurley
Electronic Ticketing Process

Old Process with Paper Ticket

Trooper takes license and registration back to cruiser
Obtains Driver License and Registration
Returns to Vehicle

Trooper

Trooper handwriting
DL info
Registration Info
Infraction Info
Trooper info, signature, badge
Carbon Copy
Paper Ticket

5 to 10 minutes per stop

Trooper processes ticket through troop stations to DMV as time permits — approximate delivery time 2—4 weeks

Trooper returns to vehicle

Returns Driver License and Registration, Issues Ticket

Returns to Vehicle

Trooper

Exits Vehicle

New Process (Reduced filing time 24 – 48 hours)

Trooper Pulls Over Motorist

Trooper takes license and registration back to cruiser.

Scans License and Registration sends data to laptop

 Trooper

Laptop

Trooper Takes ticket

Printer

Save and Print ticket

3 - 5 minutes per stop

Motorist Receives Ticket

Trooper returns to vehicle
Electronic Ticketing Current Communication Process

Trooper Downloads Stored Tickets

Laptop

Trooper can
- search for tickets
- edit their notes
- print copy for court appearance

Trooper

Download is via network connection at troop stations

E-Ticket Server

DMV can
- search for tickets
- print copies for court
- verify content on defendant copy

DMV Staff

Nightly transfer to mainframe

Mainframe Computer DMV Applications Financial Responsibility

Final Processing of Drivers License Process/Courts

Outbound

Paper Process

Courts Action for Not Guilty Pleas

Inbound

State of New Hampshire

DO IT
DEPARTMENT OF INFORMATION TECHNOLOGY

Download is via network connection at troop stations

Mainframe Computer DMV Applications Financial Responsibility

Nightly transfer to mainframe

Final Processing of Drivers License Process/Courts

Outbound

Paper Process

Courts Action for Not Guilty Pleas

Inbound

State of New Hampshire

DO IT
DEPARTMENT OF INFORMATION TECHNOLOGY
Electronic Ticketing Future Communication Process

Trooper Downloads Stored Tickets

Trooper can:
- search for tickets
- edit their notes
- print copy for court appearance

DMV can:
- search for tickets
- print copies for court
- verify content on defendant copies

Download via network (backup)

Realtime Download via *VPN and Air Card (Considering Fueling Stations as well)

Laptop

E-Ticket Server

Nightly transfer to mainframe

Final Processing of Drivers License Process/Courts

Mainframe Computer DMV Applications Financial Responsibility

* VPN = Virtual Private Network