

# 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 8<sup>th</sup>
- 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

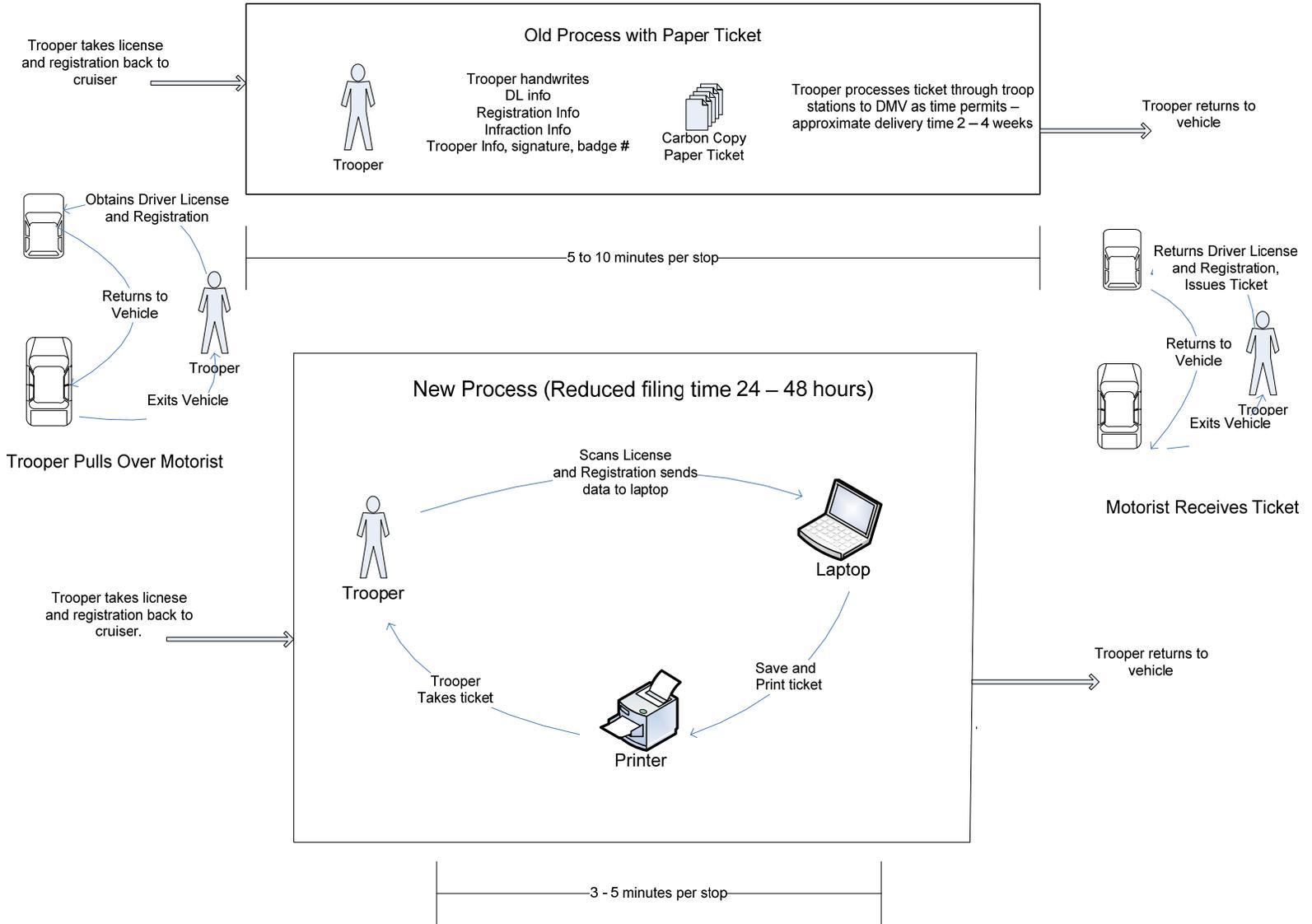
## State Police

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

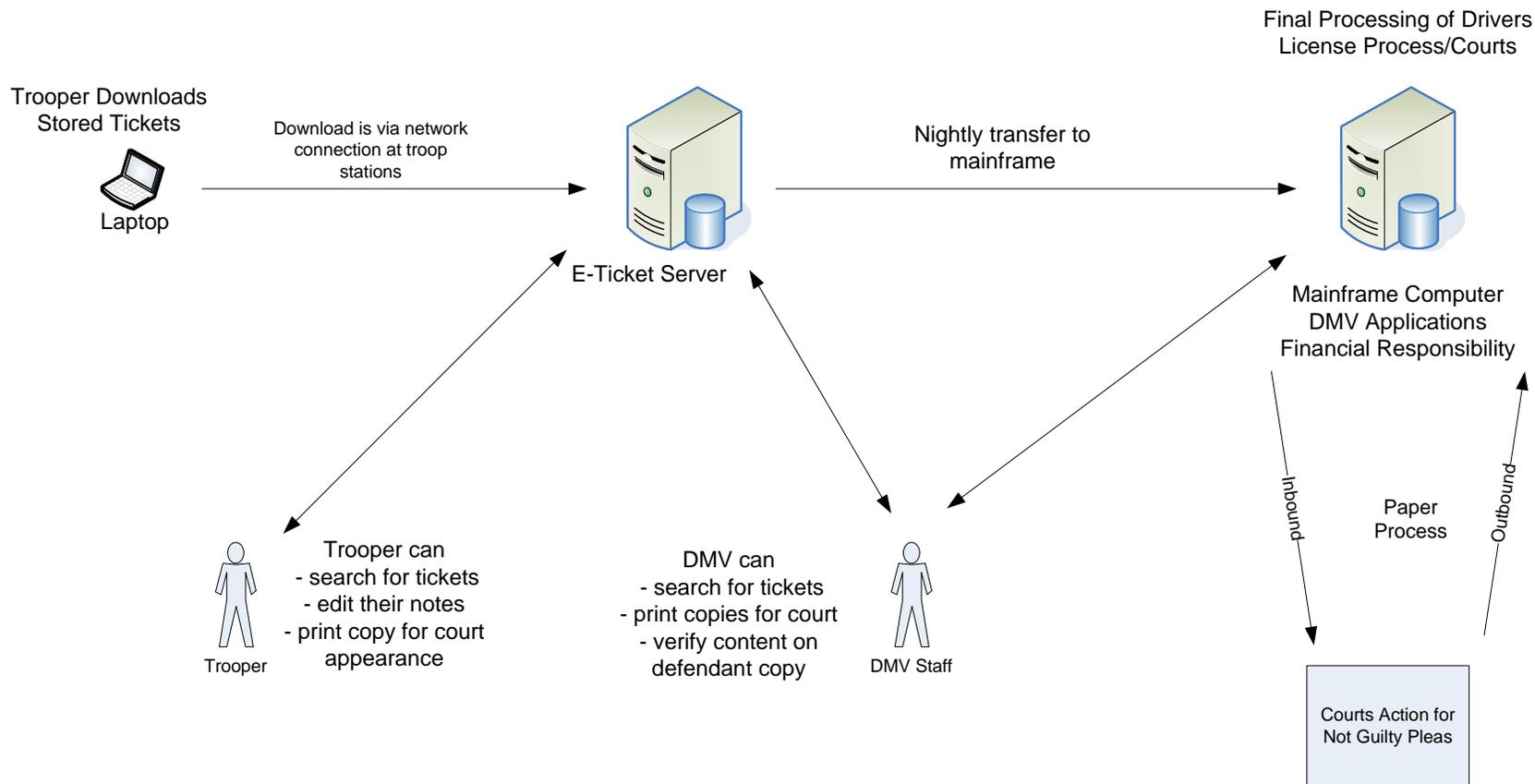
## COURTS

- Paula Hurley

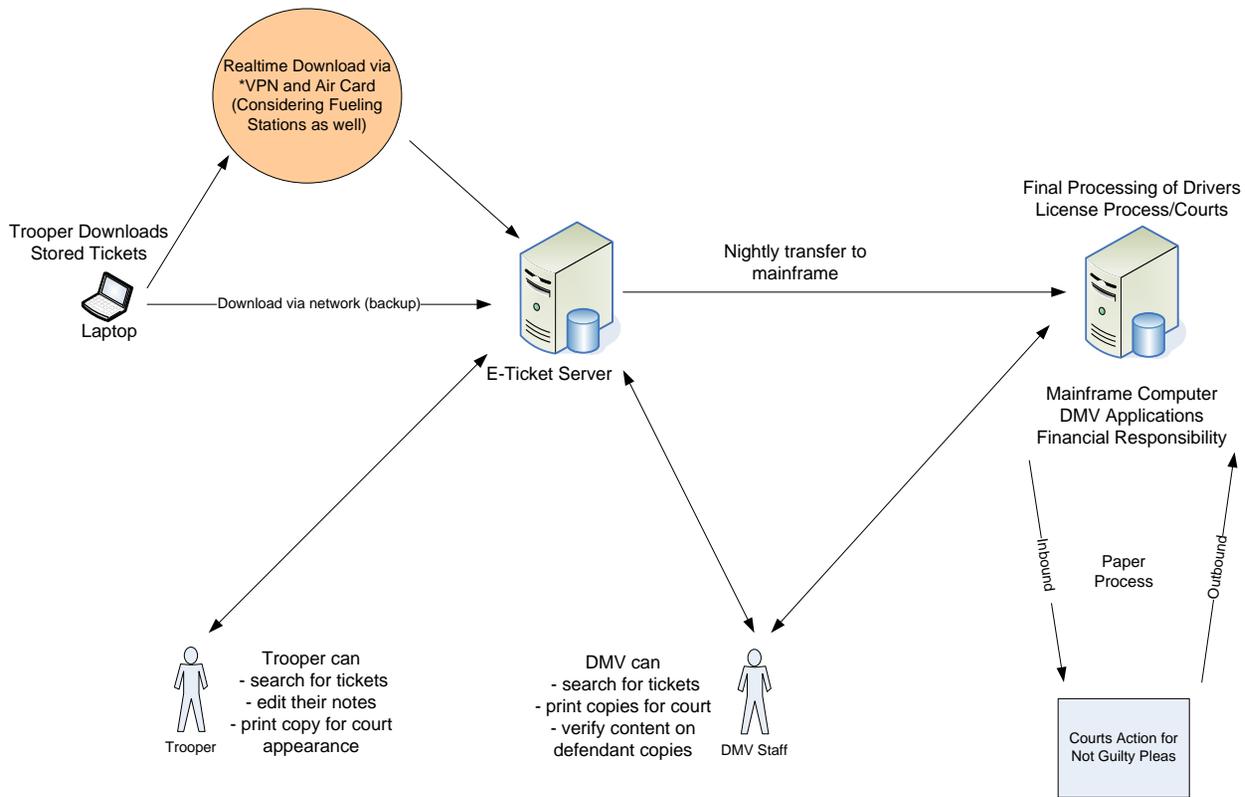
# Electronic Ticketing Process



# Electronic Ticketing Current Communication Process



# Electronic Ticketing Future Communication Process



\* VPN =Virtual Private Network