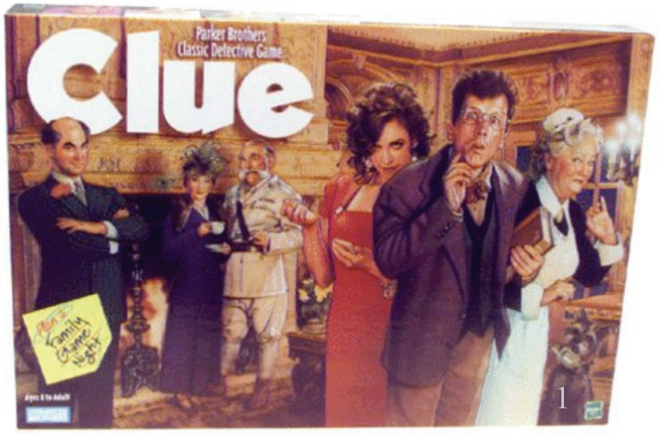
THE BIGGEST GAME OF CLUE® YOU'VE EVER PLAYED

Large Scale Problem Solving Methods
Used in
Lost Person Search Management

Don Scelza

CDS OUTDOOR SCHOOL



Incidents

- July 04 – Lost 52 YO female. Subject has history of strokes and brain damage
- September 04 – Search for two possibly abducted teenage females
- January 05 – Lost 55 YO female. High/swift water makes searching dangerous
- January 05 – Lost 6 YO autistic male. Temps at night 10-15F
- May 05 –Despondent 22 YO male recently returned from serving in the Gulf. Subject wounded by an IED
- June 05 – Lost 14 YO female. Indications were that this was a homicide search
- October 07 – 18 YO autistic male lost in the Dolly Sods Wilderness Area

Who am I ?
Why Should You Care?

President - Pennsylvania Search and Rescue Council

Incident Commander – Appalachian Search and Rescue Conference

Instructor – PA Department of Conservation and Natural Resources

Founder – CDS Outdoor School, Inc

VP Engineering Services – FORE Systems

VP Customer Service & Support - Marconi

Incidents

- September 11, 2001 – Company response to the World Trade Center and Pentagon attacks
- October 2004 - Company Web and Engineering installations hacked. Evidence of new product designs as target
- On-Going – Plan for Service Interruption Events

Covered in this Talk

- What are Large Scale Problems?
- Preplanning
- Incident Command System
- Strategy
- Tactics
- After Action
- Preventative Programs

Large scale problem solving

The problems:

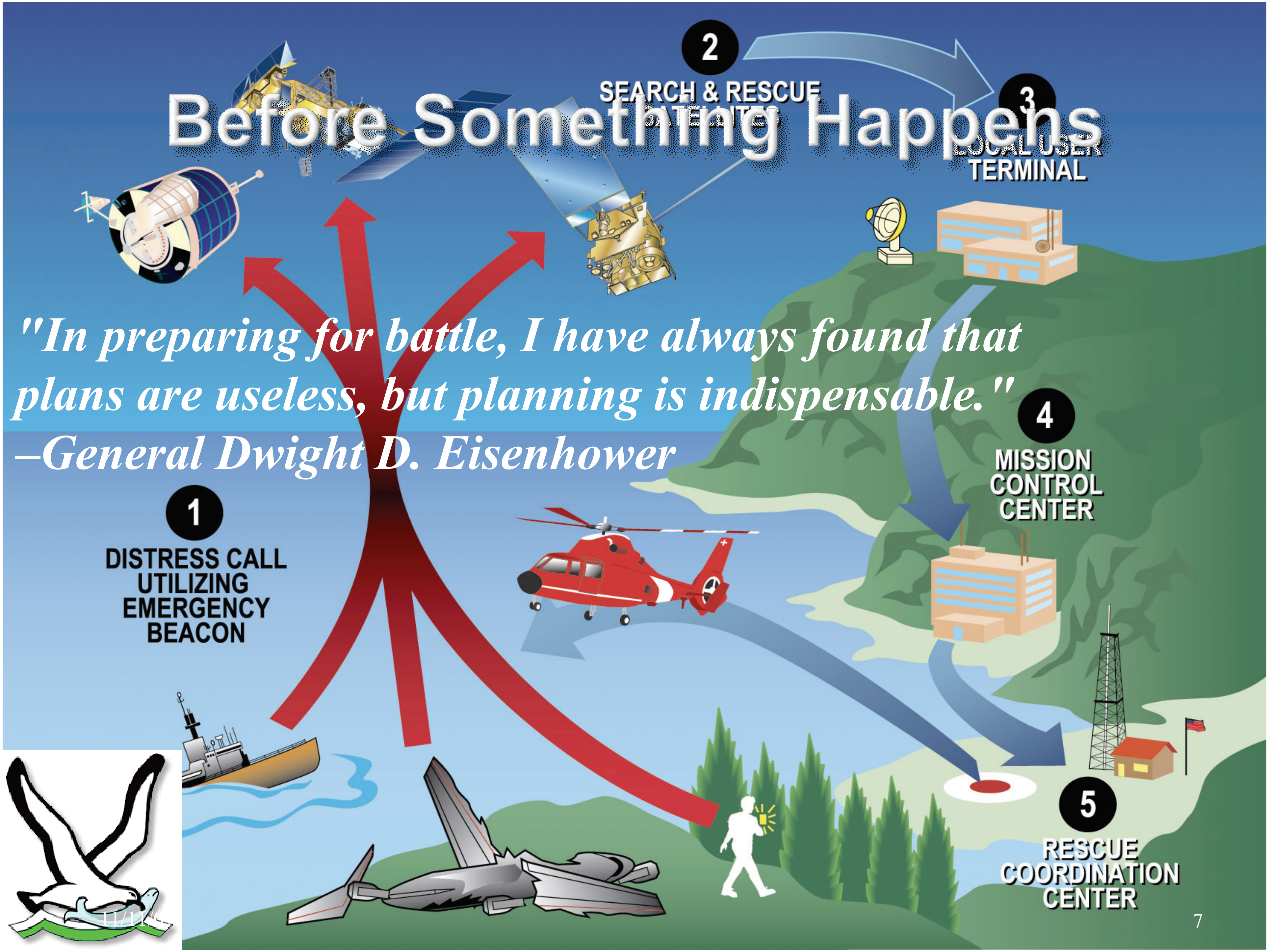
- Are time Critical
- May involve human life
- May involve property loss
- May be criminal in nature

The solutions

- Involve a large number of people
- Involve a large number of organizations
- May involve law enforcement

Before Something Happens

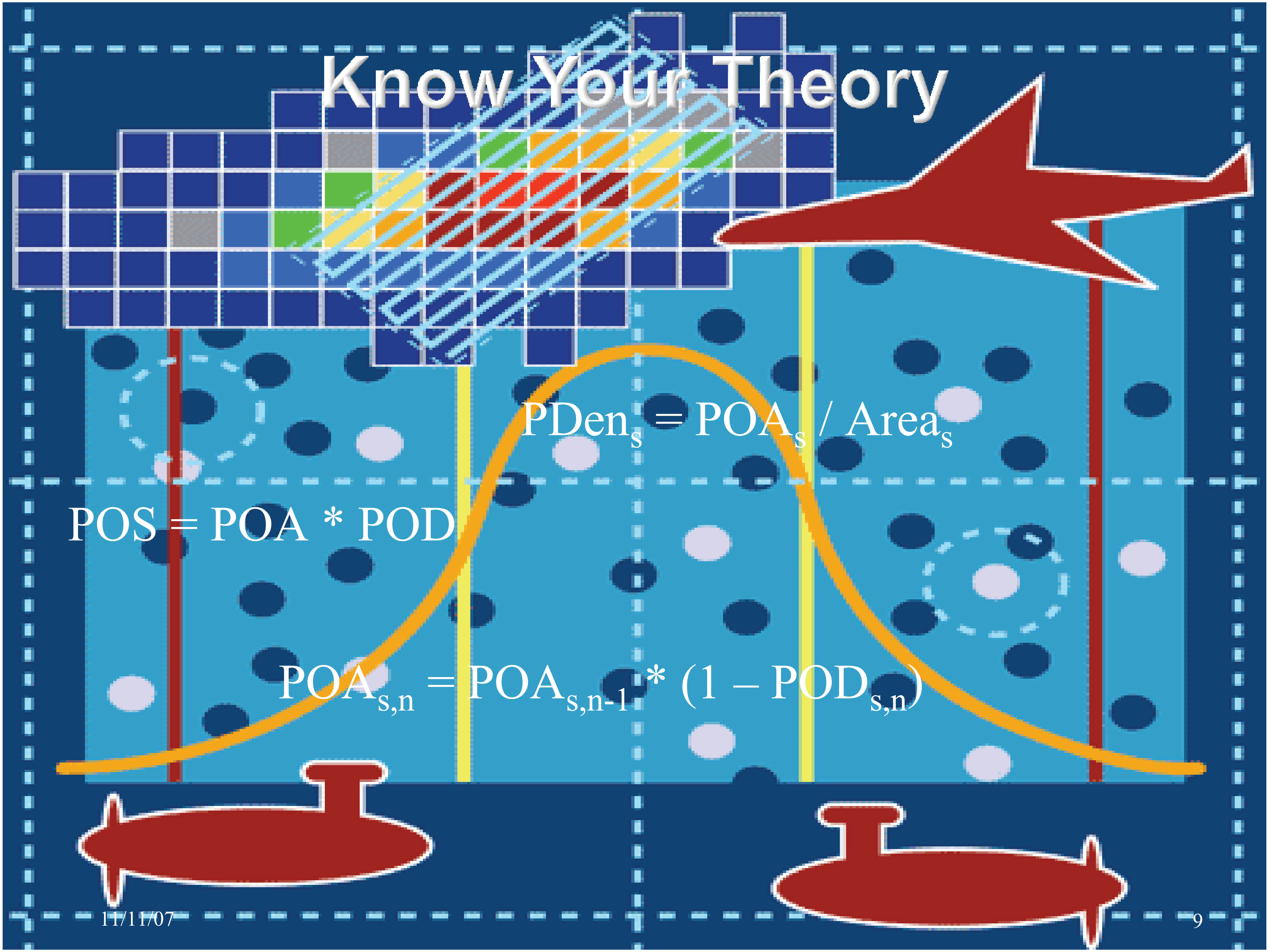
"In preparing for battle, I have always found that plans are useless, but planning is indispensable." –General Dwight D. Eisenhower


2
SEARCH & RESCUE SATELLITES
3
LOCAL USER TERMINAL
4
MISSION CONTROL CENTER
1
DISTRESS CALL UTILIZING EMERGENCY BEACON
5
RESCUE COORDINATION CENTER

Know Your History

- What types of events have taken place in this area?
- Are there characteristics in common between them?
- When similar events have taken place, is there a common solution?
- What happened last time?
- How did you fix that one?

Know Your Theory



$$PDen_s = POA_s / Area_s$$

$$POS = POA * POD$$

$$POA_{s,n} = POA_{s,n-1} * (1 – POD_{s,n})$$

The Math Behind the Search

- It’s not about lining people up shoulder to shoulder
- There is theory and accepted practice
- Probability of Area – POA

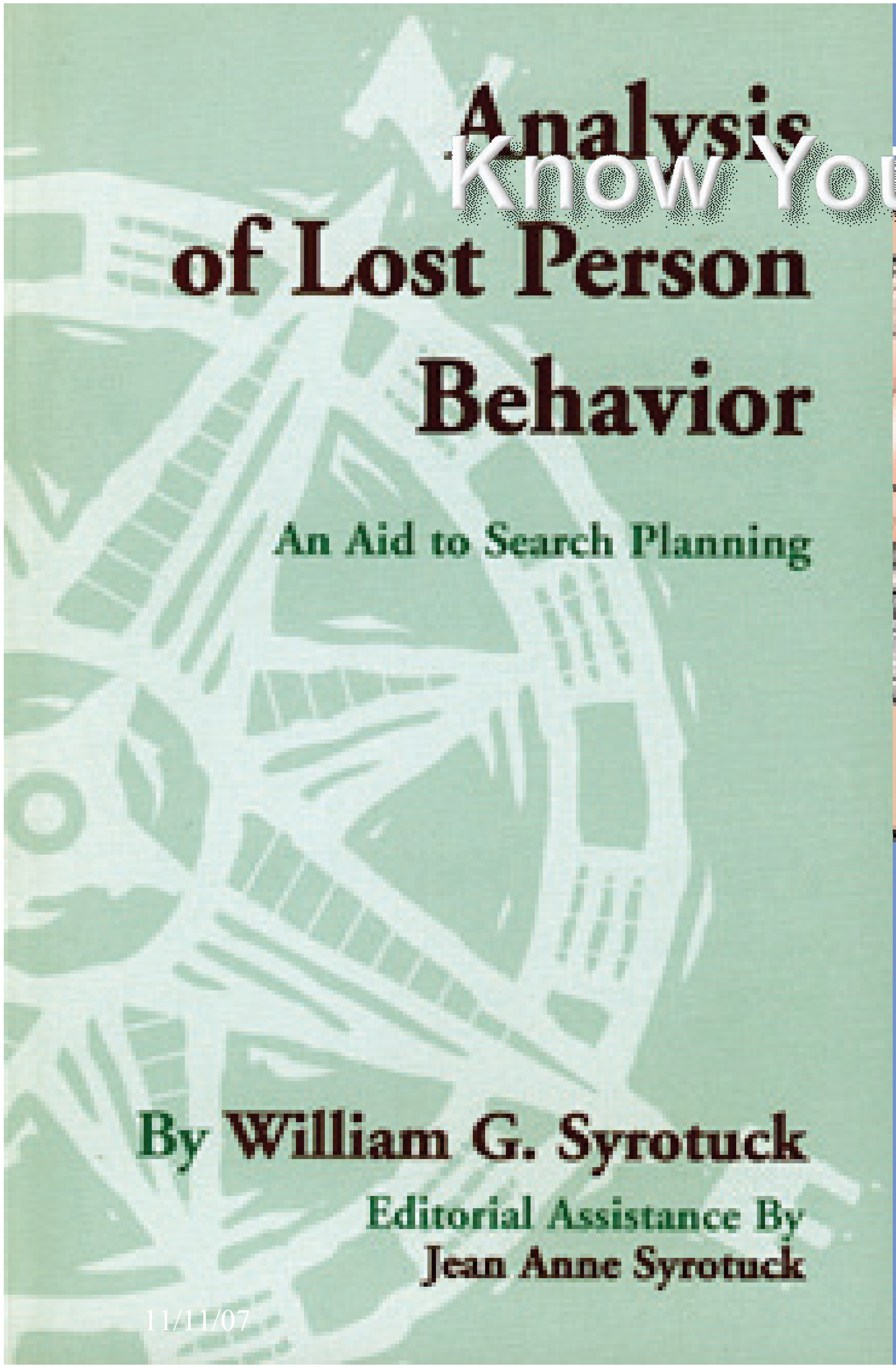
  Probability that the subject is in a specific area
- Probability of Detection – POD

  Probability that if a subject/clue was in the area the searcher would have found it
- Probability of Success – POS

  Duh

$$\mathrm{POS} = \mathrm{POA} * \mathrm{POD}$$

Know Your Subject

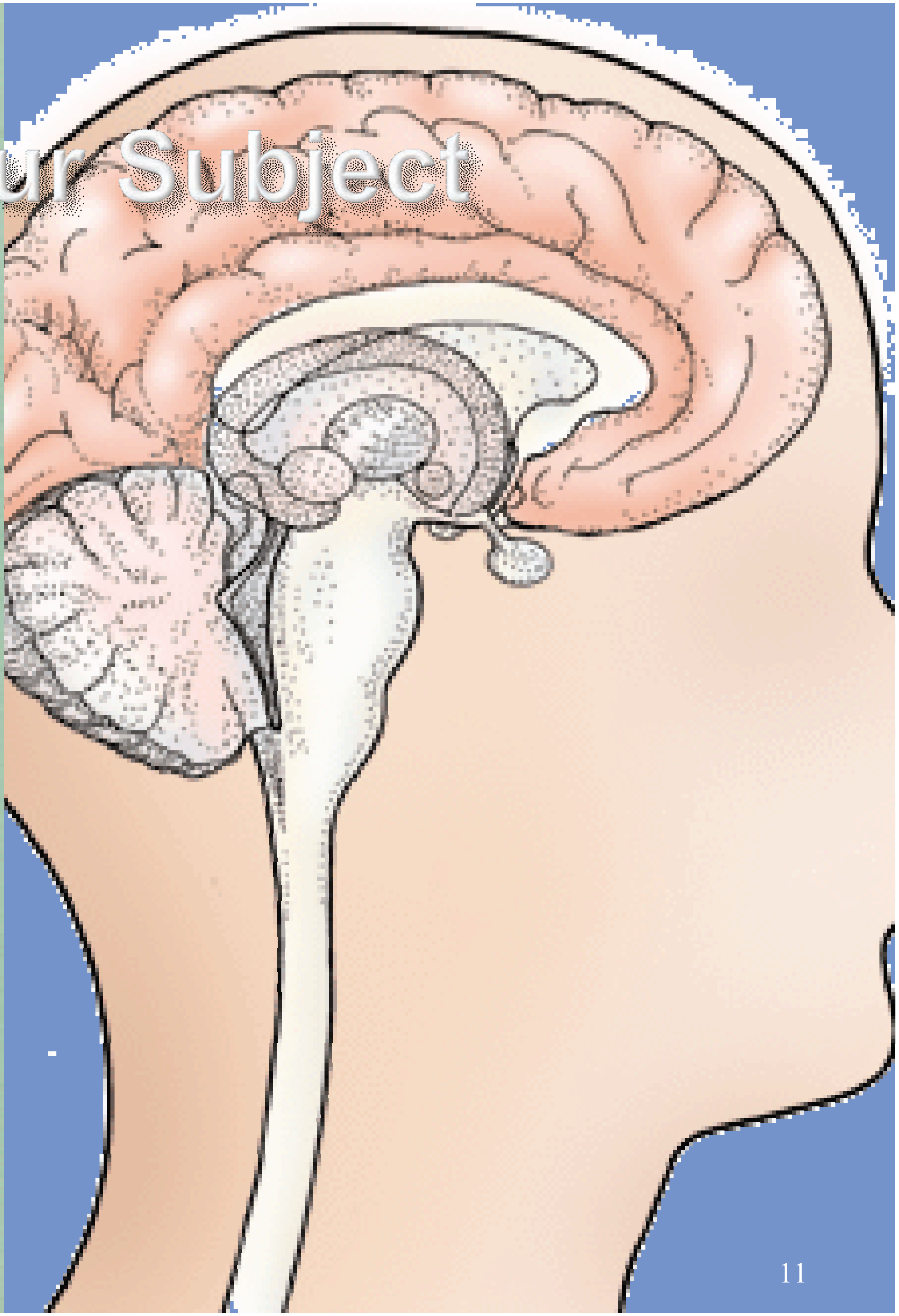


Analysis of Lost Person Behavior

An Aid to Search Planning

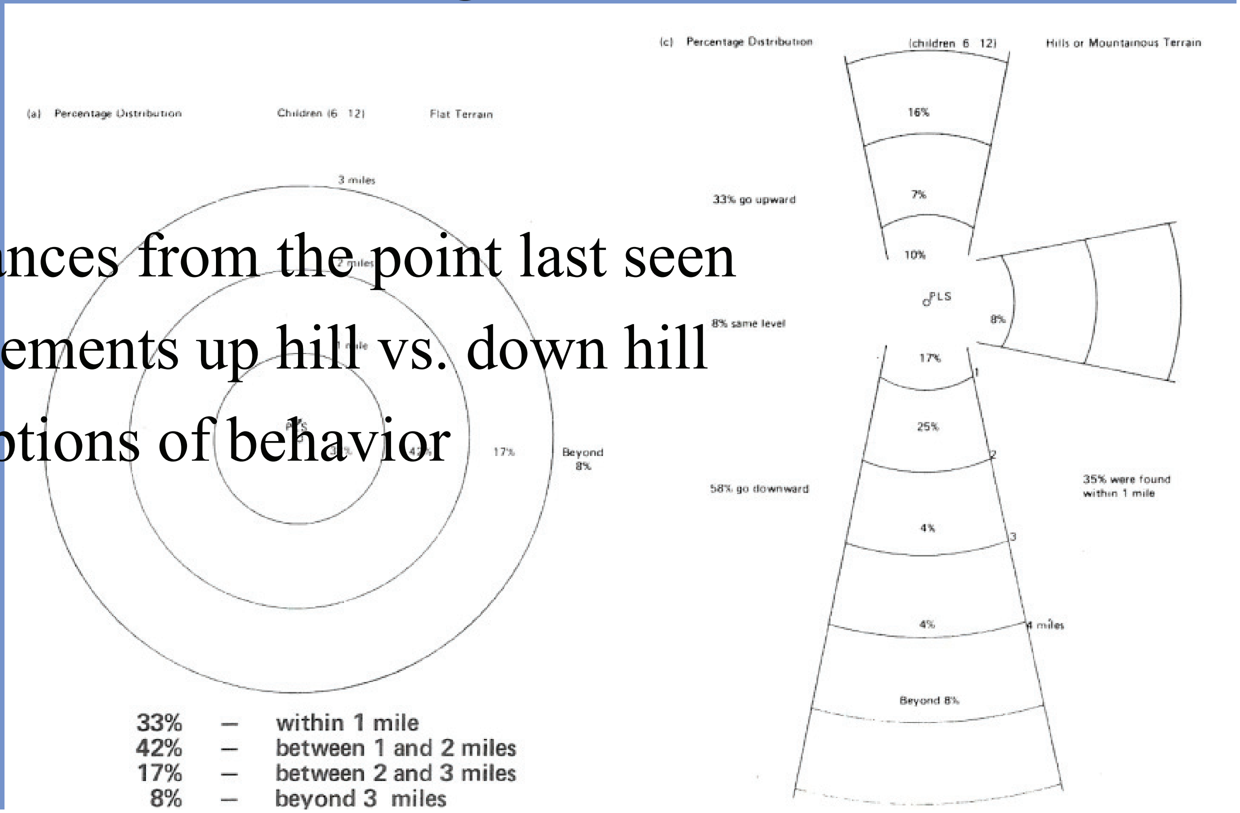
By William G. Syrotuck

Editorial Assistance By
Jean Anne Syrotuck

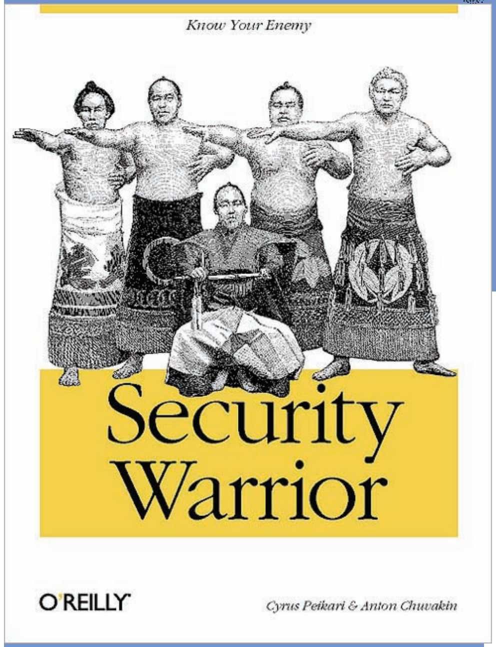


Lost Person Behavior

- A statistical study of what a class of subjects is likely to do when lost
- Provides help with determining initial values of POA
- It gives
  - Percentile distances from the point last seen
  - Percentile movements up hill vs. down hill
  - General descriptions of behavior



Know YOUR Theory

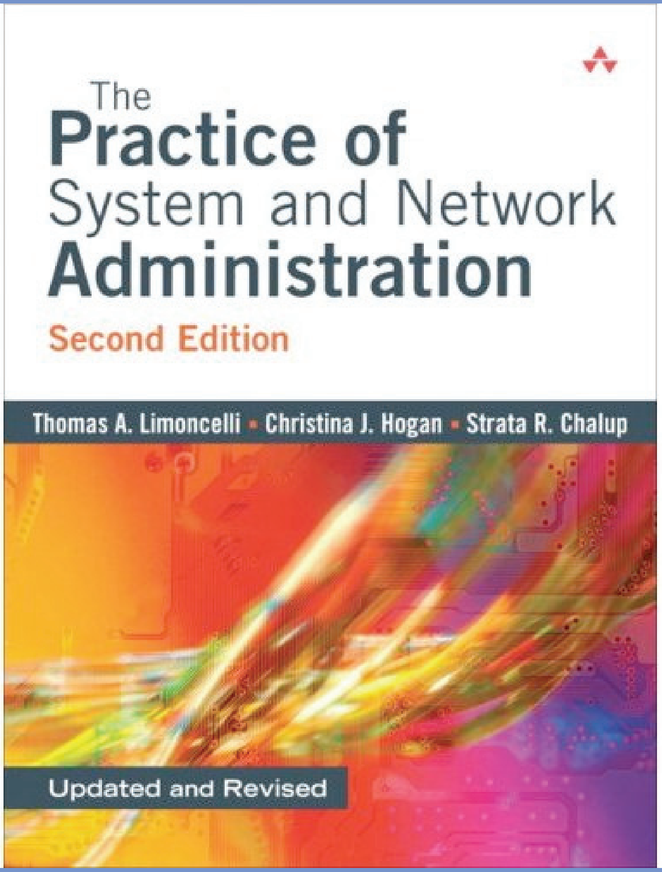


Know Your Enemy

Security Warrior

O'REILLY

Cyrus Peikari & Anton Chuvakin

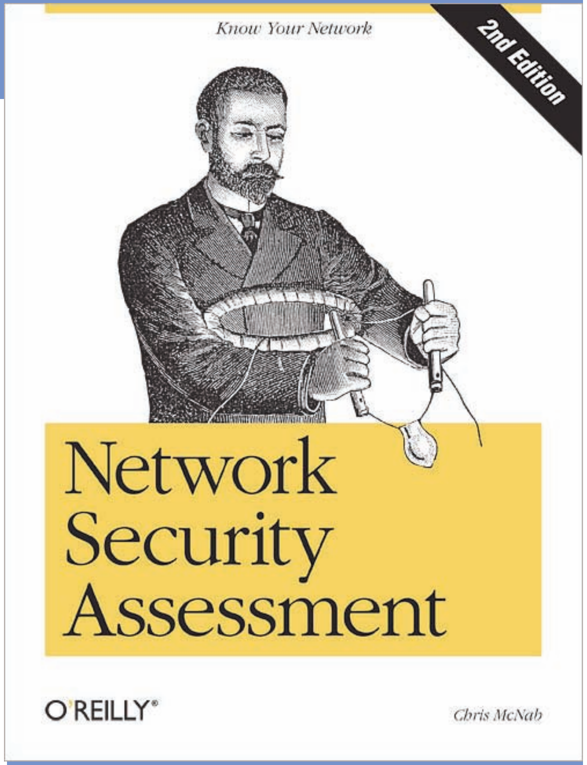


The Practice of System and Network Administration

Second Edition

Thomas A. Limoncelli • Christina J. Hogan • Strata R. Chalup

Updated and Revised



Know Your Network

2nd Edition

Network Security Assessment

O'REILLY®

Chris McNab

What Theory Covers Your Area?

- Security Policies?
- Distributed Systems?
- OS Design
- Performance Monitoring?
- Emergent Behavior?
- User Psychology?

Know Your Resources

11/11/07

Resources

- Know what certifications your resources have
- Know how to get them
- Know their response time
- Cost

Ground Searchers

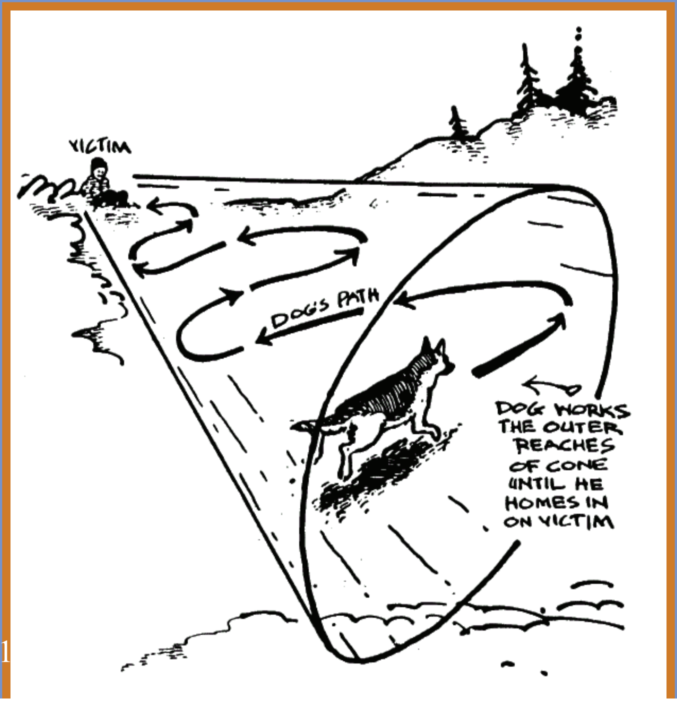
Ground Resources

- Hasty Searchers
  - Used early in the search
  - High speed
  - High efficiency
  - Low thoroughness
- Grid Searchers
  - Used later in the search
  - Slower
  - Less efficient
  - High thoroughness
- Man Trackers
  - Used when clues are found
  - Highly trained
  - Very slow
  - Very high thoroughness
- Investigators
  - Used throughout the event
  - Highly trained
  - Look for clues that can be used to direct the search

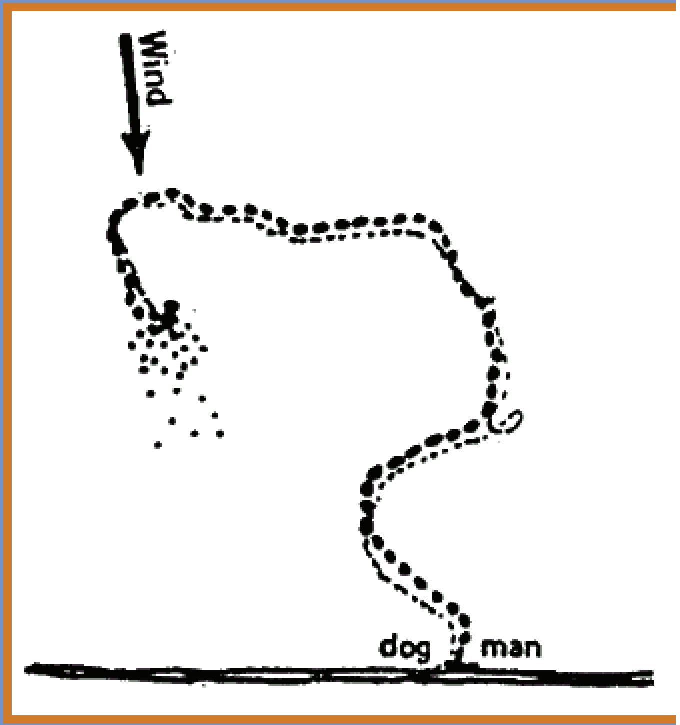
Dog Searchers

Dog Resources

- Air Scent Dogs


VICTIM
DOG'S PATH
DOG WORKS THE OUTER REACHES OF CONE UNTIL HE HOMES IN ON VICTIM

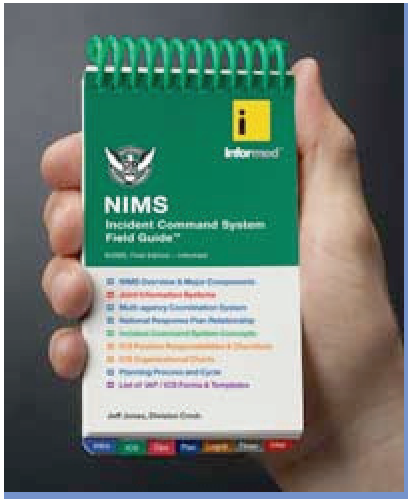
- Track/Trailing Dogs



Aircraft Searchers

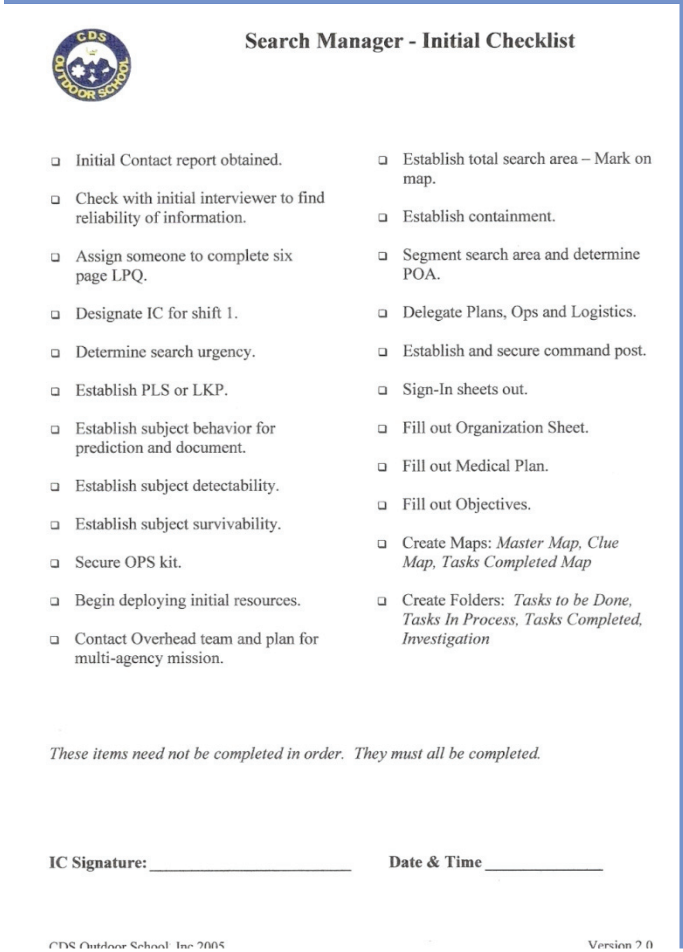
Aircraft Resources

- Fixed wing aircraft fly fast so they don’t see a lot
- Rotary wing aircraft can fly slower and hover
- Some aircraft have special tools
  - FLIR – Forward Looking InfraRed
  - Spectral Analysis
- You have to be able to land and fuel them



Other Resources

NATIONAL WILDFIRE COORDINATING GROUP



Search Manager - Initial Checklist

- ❑ Initial Contact report obtained.
- ❑ Check with initial interviewer to find reliability of information.
- ❑ Assign someone to complete six page LPQ.
- ❑ Designate IC for shift 1.
- ❑ Determine search urgency.
- ❑ Establish PLS or LKP.
- ❑ Establish subject behavior for prediction and document.
- ❑ Establish subject detectability.
- ❑ Establish subject survivability.
- ❑ Secure OPS kit.
- ❑ Begin deploying initial resources.
- ❑ Contact Overhead team and plan for multi-agency mission.
- ❑ Establish total search area – Mark on map.
- ❑ Establish containment.
- ❑ Segment search area and determine POA.
- ❑ Delegate Plans, Ops and Logistics.
- ❑ Establish and secure command post.
- ❑ Sign-In sheets out.
- ❑ Fill out Organization Sheet.
- ❑ Fill out Medical Plan.
- ❑ Fill out Objectives.
- ❑ Create Maps: *Master Map, Clue Map, Tasks Completed Map*
- ❑ Create Folders: *Tasks to be Done, Tasks In Process, Tasks Completed, Investigation*

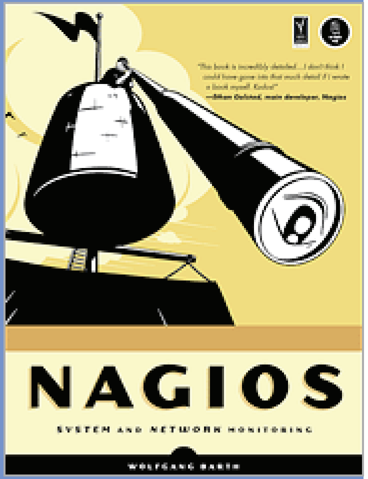
These items need not be completed in order. They must all be completed.

IC Signature: ______________________ **Date & Time** _____________

CDS Outdoor School, Inc 2005 Version 2.0

Know YOUR Resources

First Responders Guide to Computer Forensics



Handbook for Computer Security Incident Response Teams (CSIRTs)

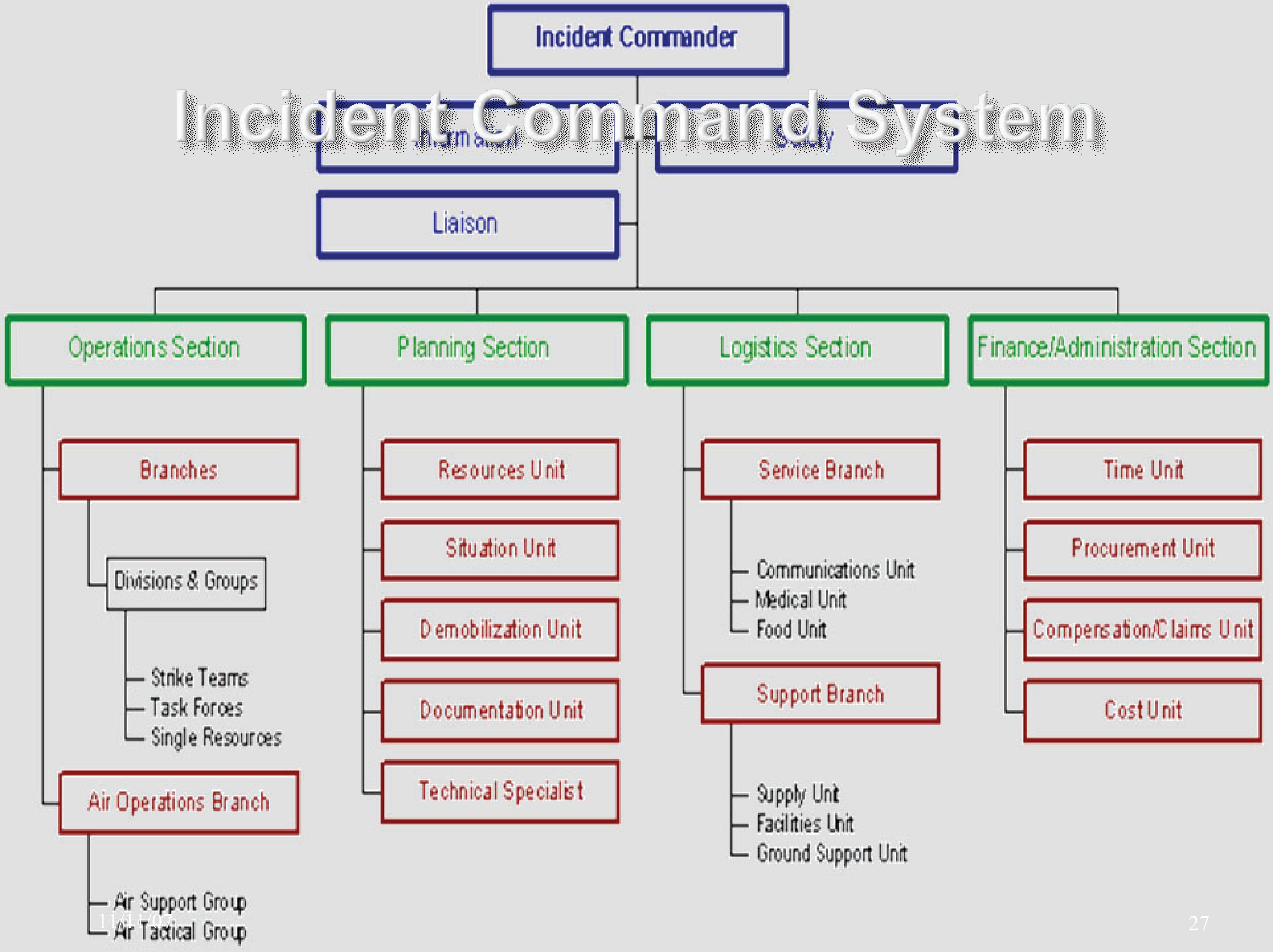
What are YOUR resources?

- Computer security experts?
- OS experts?
- Networking experts?
- Equipment Manufacturers?
- CERT?
- FBI?

The Game is On

PROFESSOR PLUM
MRS. WHITE
MR. GREEN
CANDLESTICK
WRENCH
ROPE
MRS. PEACOCK
MISS SCARLETT
COLONEL MUSTARD
REVOLVER
KNIFE
LEAD PIPE

Incident Command System



ICS a.k.a. NIMS

- The Incident Command System is used to create a management structure
- The Incident Commander is at the top
- Common terminology and common positions make it easy for people to slide into positions
- Staff Positions
  - Safety
  - PIO
  - Liaison
- Sections
  - Plans
  - Ops
  - Logistics
  - Finance

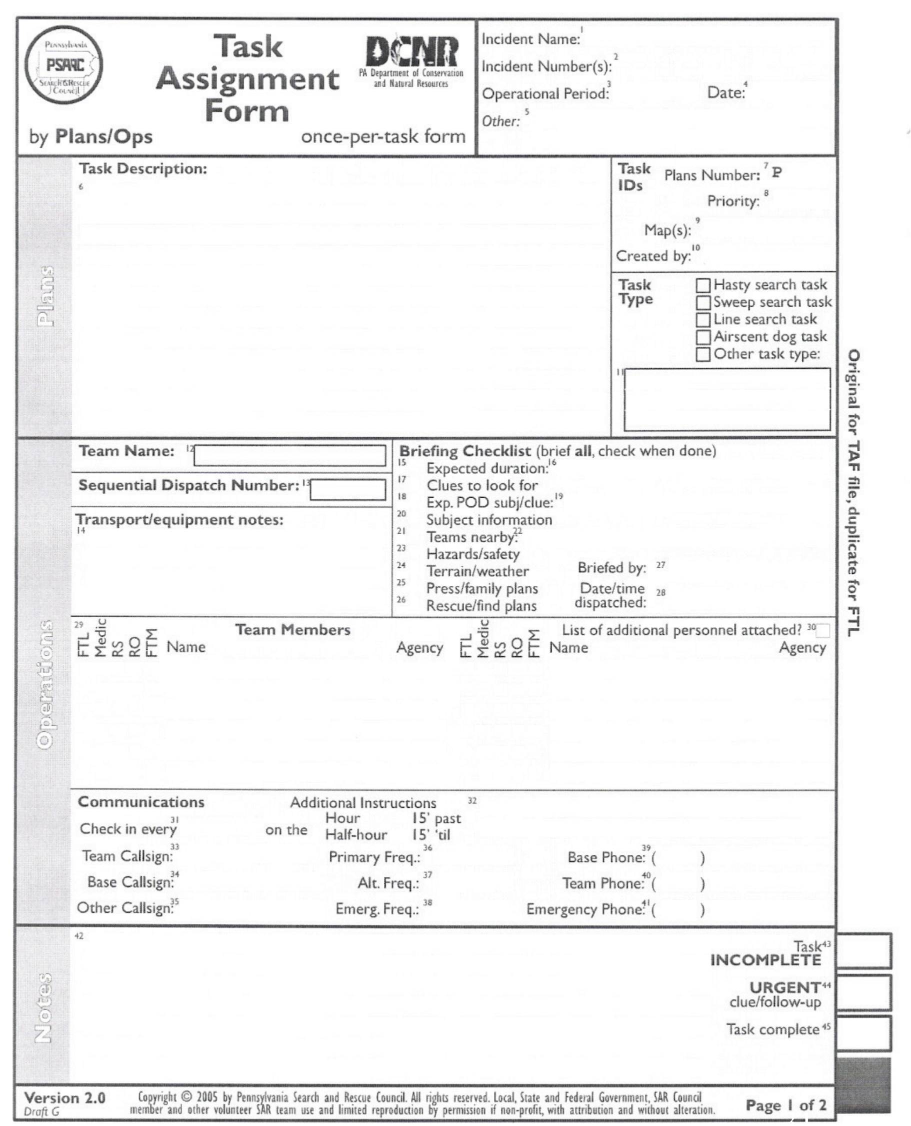
Plans – Providing Strategy

Plans

- Plans takes the objectives provided by the Incident Command and turns them into a strategy
- They are often looking 12 hours ahead
- They create the Task Assignment Form
- They take information from task execution and crunch the numbers
  - Cumulative POD $\mathrm{POD}_n = 1- (\mathrm{POD}_{n-1} * \mathrm{POD}_{s,n})$
  - Shifting POA's $\mathrm{POA}_{s,n} = \mathrm{POA}_{s,n-1} * (1 – \mathrm{POD}_{s,n})$
- They follow up on clues!

A Word about the TAF

- This form defines each specific field task
- It is created by Plans
- Executed by Ops
- Results are reviewed by Plans



Task Assignment Form

Pennsylvania PSARC Search & Rescue Council

DCNR PA Department of Conservation and Natural Resources

by **Plans/Ops** once-per-task form

Incident Name:[1]

Incident Number(s):[2]

Operational Period:[3] Date:[4]

Other:[5]

Plans

Task Description:

[6]

Task IDs Plans Number:[7] P

Priority:[8]

Map(s):[9]

Created by:[10]

Task Type

□ Hasty search task
□ Sweep search task
□ Line search task
□ Airscent dog task
□ Other task type:

[11] □

Operations

Team Name: [12] □

Sequential Dispatch Number:[13] □

Transport/equipment notes:

[14]

Briefing Checklist (brief **all**, check when done)

15 Expected duration:[16]
17 Clues to look for
18 Exp. POD subj/clue:[19]
20 Subject information
21 Teams nearby:[22]
23 Hazards/safety
24 Terrain/weather
25 Press/family plans
26 Rescue/find plans

Briefed by: [27]

Date/time dispatched: [28]

[29] **Team Members** List of additional personnel attached? [30] □

FTL	Medic	RS	RO	FTM	Name	Agency	FTL	Medic	RS	RO	FTM	Name	Agency

Communications

Check in every[31] on the Hour / Half-hour 15' past / 15' 'til

Additional Instructions [32]

Team Callsign:[33] Primary Freq.:[36] Base Phone:[39] ( )

Base Callsign:[34] Alt. Freq.:[37] Team Phone:[40] ( )

Other Callsign:[35] Emerg. Freq.:[38] Emergency Phone:[41] ( )

Notes

[42]

Task[43] **INCOMPLETE** □

URGENT[44] clue/follow-up □

Task complete[45] □

Original for TAF file, duplicate for FTL

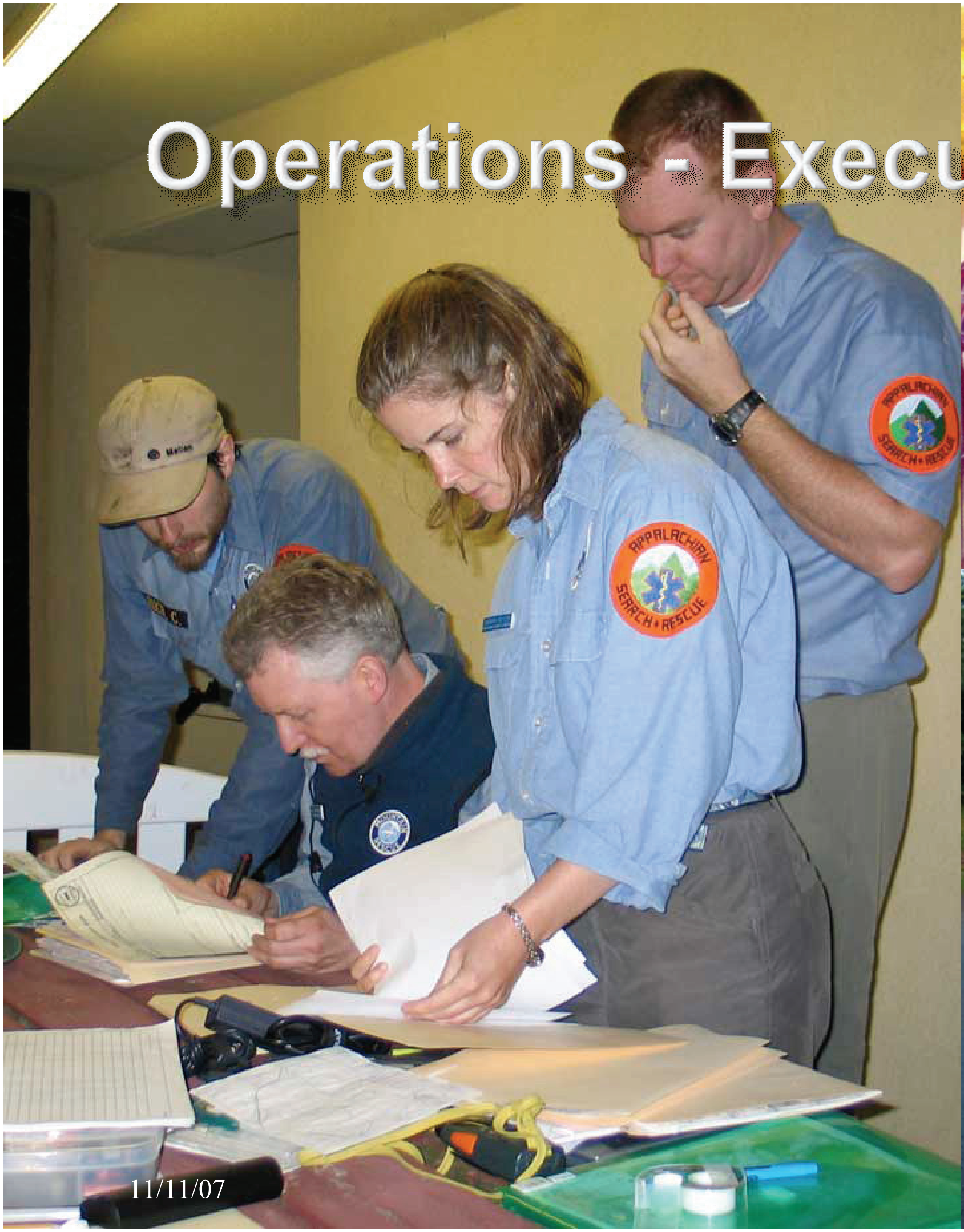
Version 2.0 *Draft G*

Page 1 of 2

Briefings

- Everyone in the operation wants to know what is going on
- You have to keep them up-to-date about general operations
- Specific briefings
  - Full team Briefing
  - FTL Briefing
  - FTL Debriefing
  - Press Briefing
  - IS Briefings
  - Change of Staff

Operations - Executing Tactics



Operations

- Ops takes the strategy provided by Plans and makes it happen
- They “execute” the TAF
- They brief the field teams on what needs to be done
- They debrief the field teams to find out what was done
- They provide information to Plans about “interesting” events a.k.a Clues

Oh yeah, About those clues

- There are usually lots and lots of clues
  - Some are interesting
  - Most are not
- All clues are logged by Comms
- If they are significant they are brought to Ops & Plans attention immediately
- The IC must sign off on all clue actions
- The occurrence of a significant clue changes the POA of the area where it was found

Management Resources

- Know who is good in Plans and who is good in Ops
  - They are different types of people
  - Plans people like to work in methodical, quiet, slow environments
  - Ops people like to be in the middle of the action
- Know who is good at logistics
  - Locals
  - People who are good at “getting” things
- Pick your PIO and Liaison Officer carefully

Using ICS in YOUR Incident

- Put a command structure in place
- Standard Terminology – *A Common Language for Computer Security Incidents* – Sandia National Laboratories
- Response Teams – *Defining Computer Security Incident Response Teams* – CMU
- Officers
  - Safety
  - PIO
- Sections
  - Plans
  - Ops
  - Logistics

After Action

- There should be a review of the actions taken during the event
- What went well?
- What went poorly?
- What should be changed in the preplan?
- What data needs to get cycled into the history & statistics?
- Could this have been prevented?

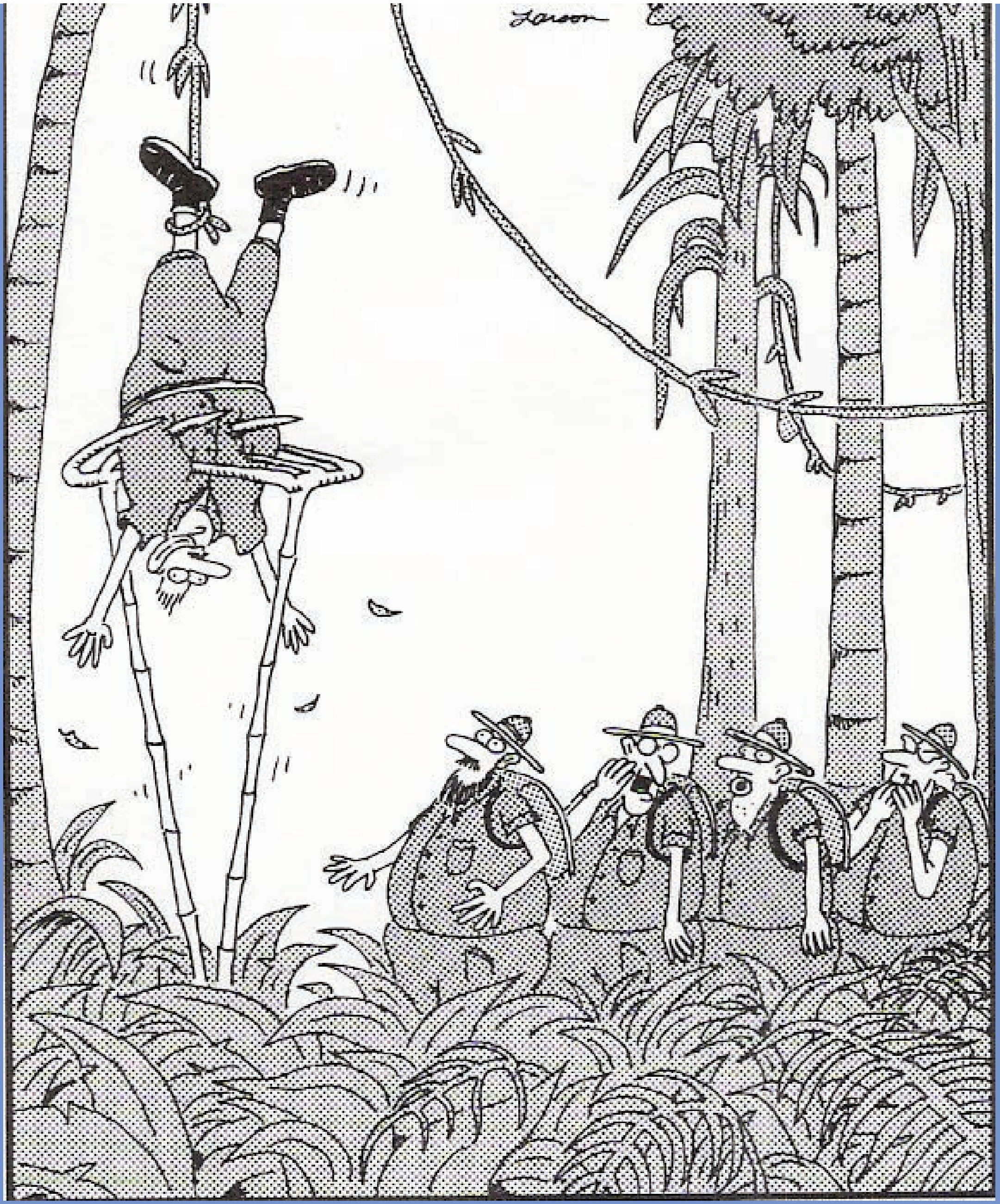
Preventative Efforts

Hug A Tree

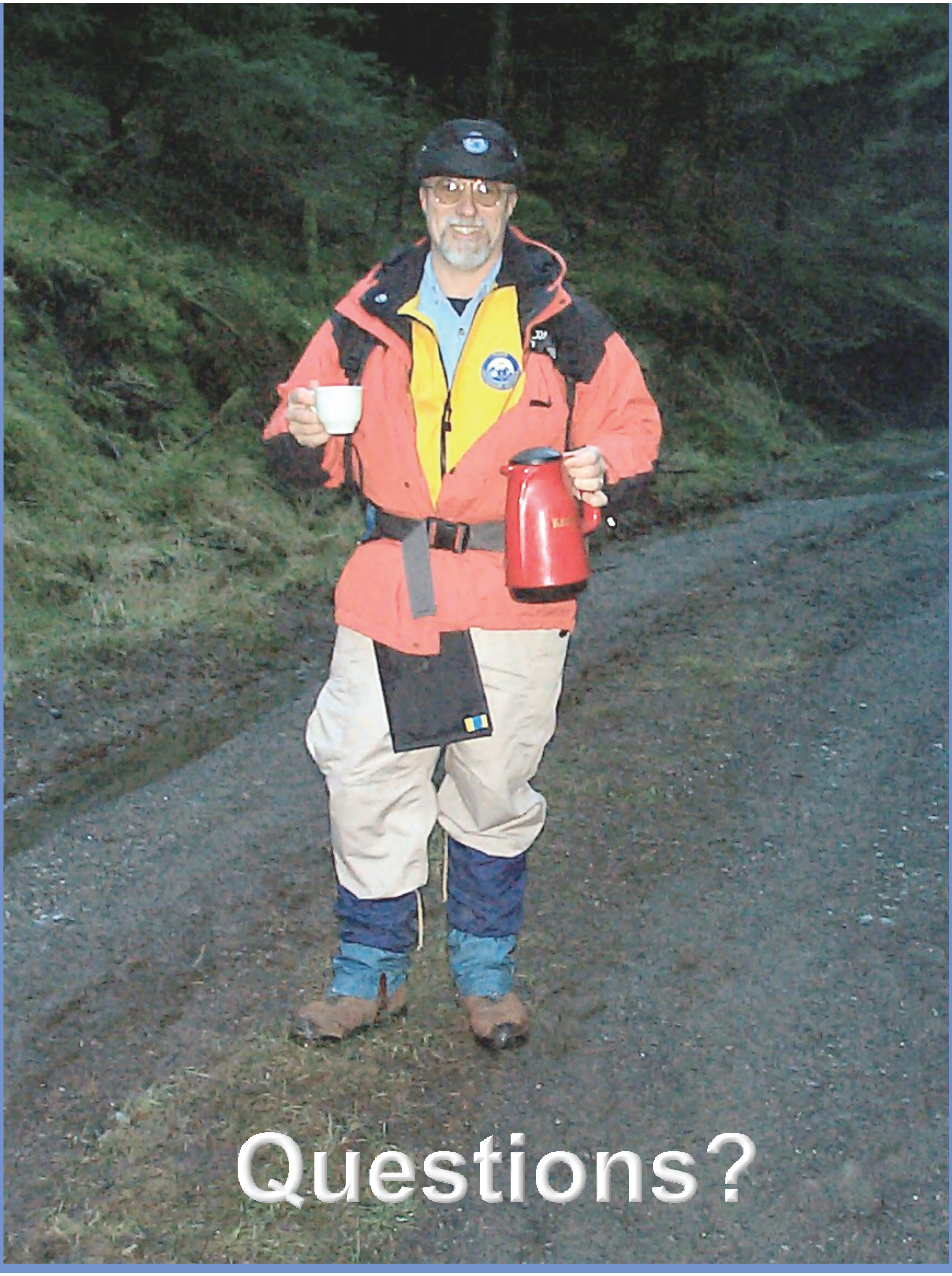
- February 1981, 9 year old Jimmy Beveridge became lost. After four days Jimmy's body was found approximately two miles from the campsite.
- After this mission Ab Taylor created the Hug-A-Tree and Survive program
- Aimed at teaching children what to do when they get lost
- Taught throughout the US and Canada at no cost

What are YOUR Preventative Actions?

- System security tests?
- Infrastructure tests?
  - Backup power?
  - Fire suppression?
- Physical Security?
- HR policies?



That’s Why I Stay in Base



Questions?