

Telephony Denial of Service Attacks

Altoona, Iowa ■ November 4, 2014



**Homeland
Security**

**Jim Lundsted
Regional Coordinator, OEC**

Office of Emergency Communications

Support and promote communications for emergency responders and government officials during all hazards and threats.

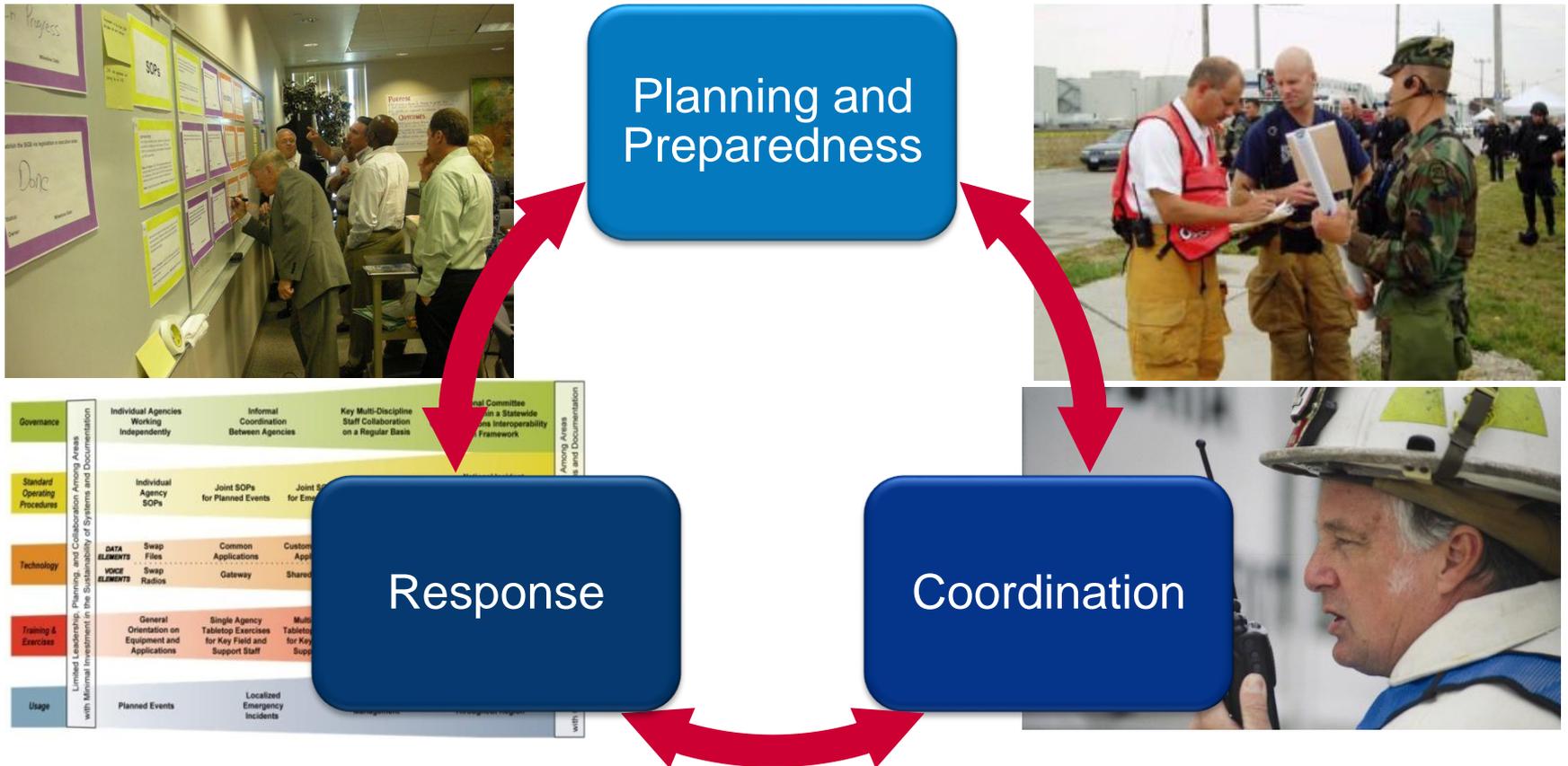


Homeland
Security

Office of Emergency Communications

Mission

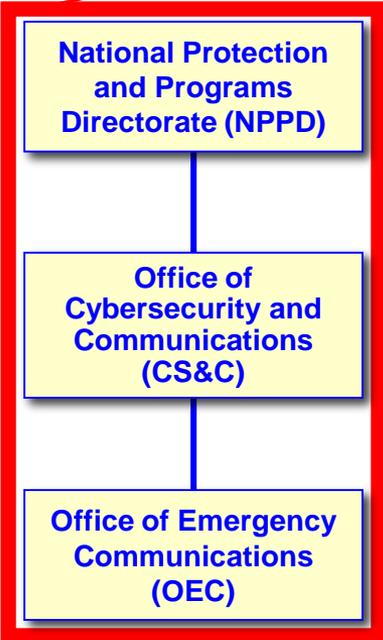
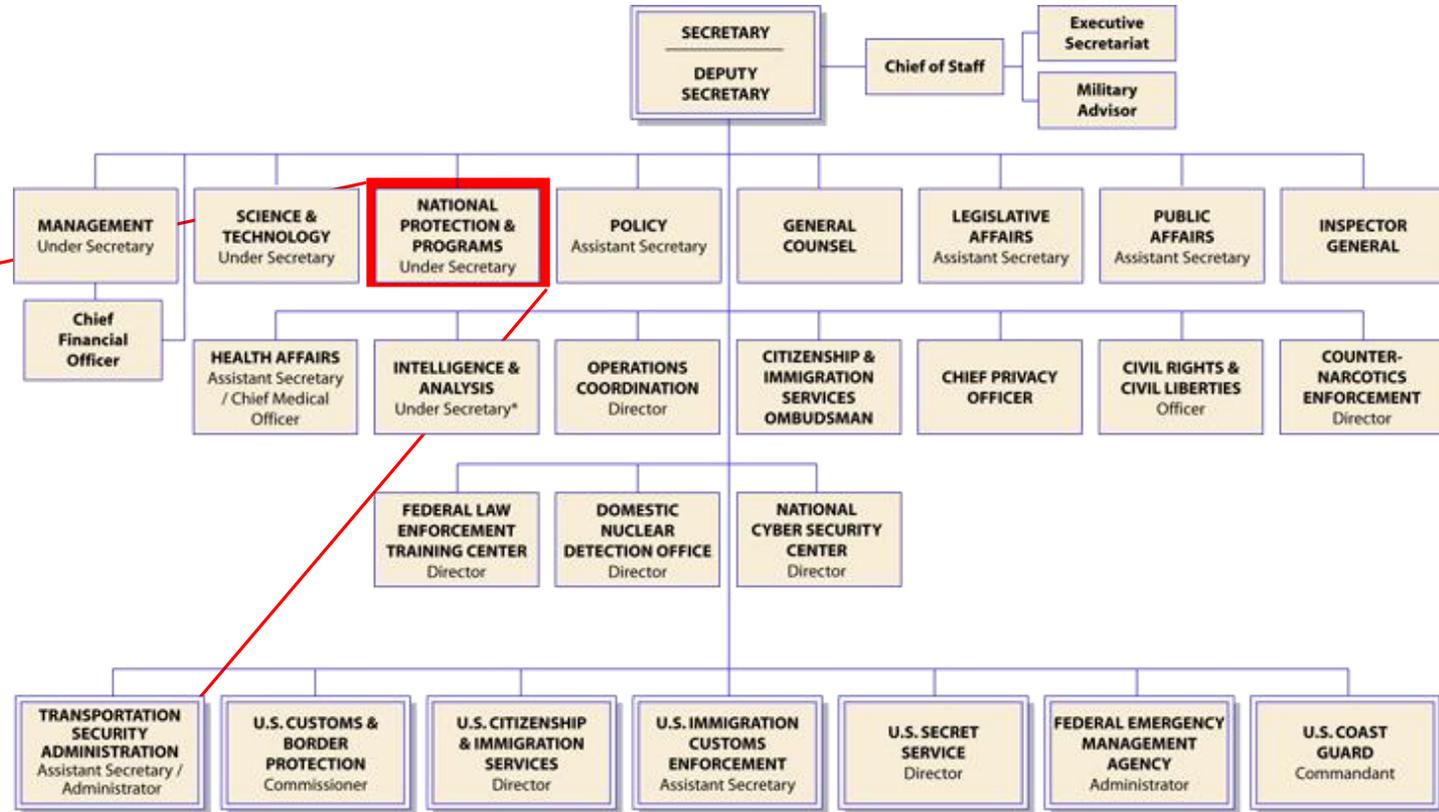
The Office of Emergency Communications (OEC) supports and promotes communications capabilities used by emergency responders and government officials to keep America safe, secure, and resilient.



Homeland Security

Office of Emergency Communications

Department of Homeland Security



What is a Denial of Service Attack?

- Denial of Service (DoS) attacks attempt to prevent legitimate users from access to information or services. You may be unable to access resources such as e-mail, Website, on-line access or other services that rely on the affected computer. The most common DoS example is “flooding” a Web site (web server/services) with requests.



What is a Denial of Service Attack?

- Distributed Denial of Service (DDoS) attacks occur when multiple computers are used to attack other computers or Web sites. Compromised computers are used to overwhelm the victim site or network.



What is a Telephony Denial of Service Attack?

- A newer type of DoS attack is called a Telephony Denial of Service (TDoS) attack. A TDoS attack attempts to “flood” the victim with a series of calls – either simultaneously or back-to-back-to-back to prevent a call center (in our case, a PSAP) from being able to perform its core functions. Both recorded messaging and “crowd sourced” types of dialing attacks have been documented.



What is a Telephony Denial of Service Attack?

- TRADITIONAL forms of telephone security/fraud have been focused on toll fraud, social engineering (sharing account information/passwords), modem or network abuse.
- We need to also prepare for a different threat: denial of service attacks against our call centers and PSAP(s).

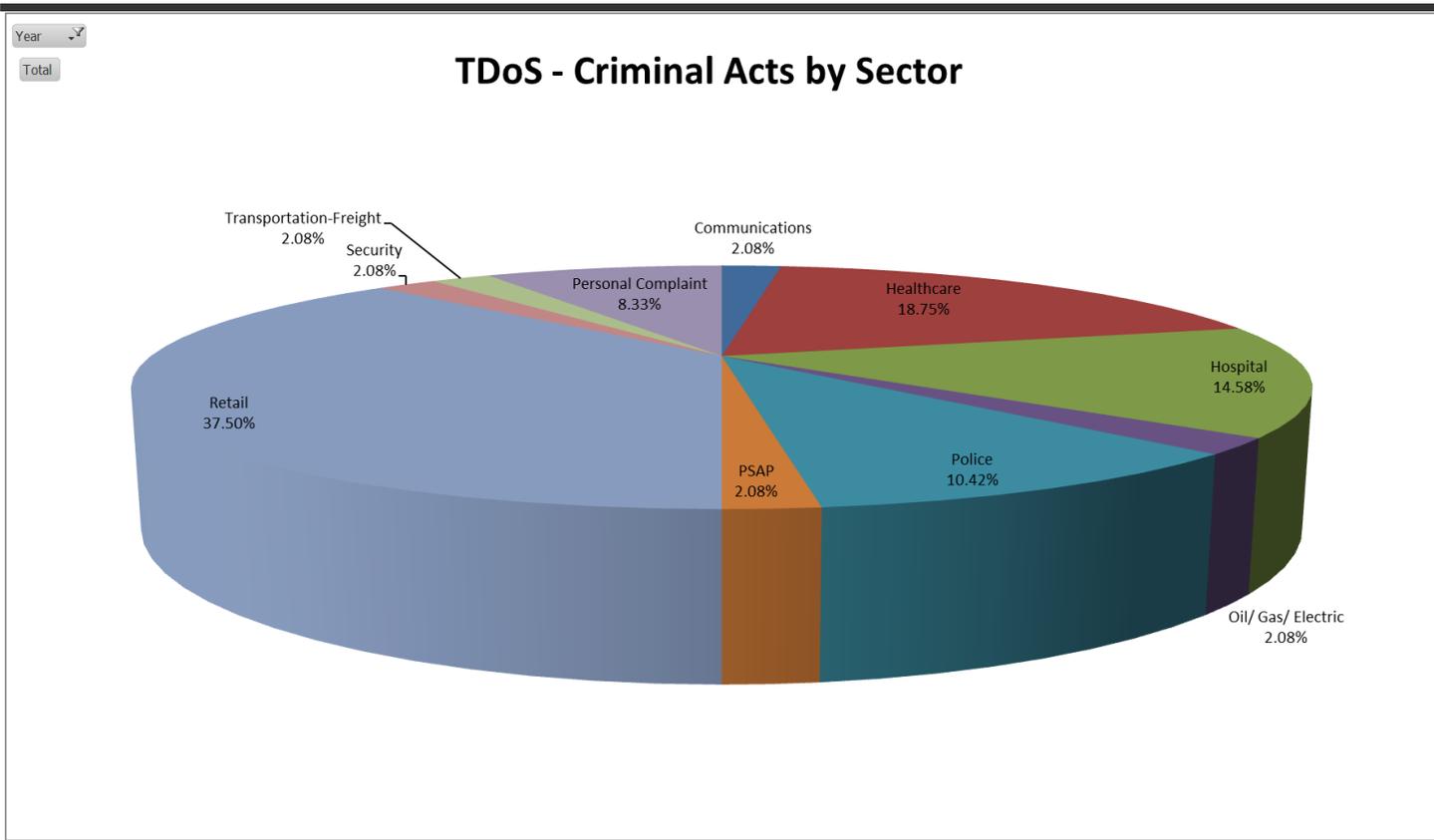


What is a Telephony Denial of Service Attack?

- Today's Threat
 - PSAP or agency's trunks are flooded with calls in an extortion attempt
 - PSAP or agency's internal IT network is compromised, causing voice service(s) issues
 - PSAP is flooded with pocket dialed, malicious, sub-adult or impaired adults dialing wireless 9-1-1 wireless from a non-service initiated (NSI) handset



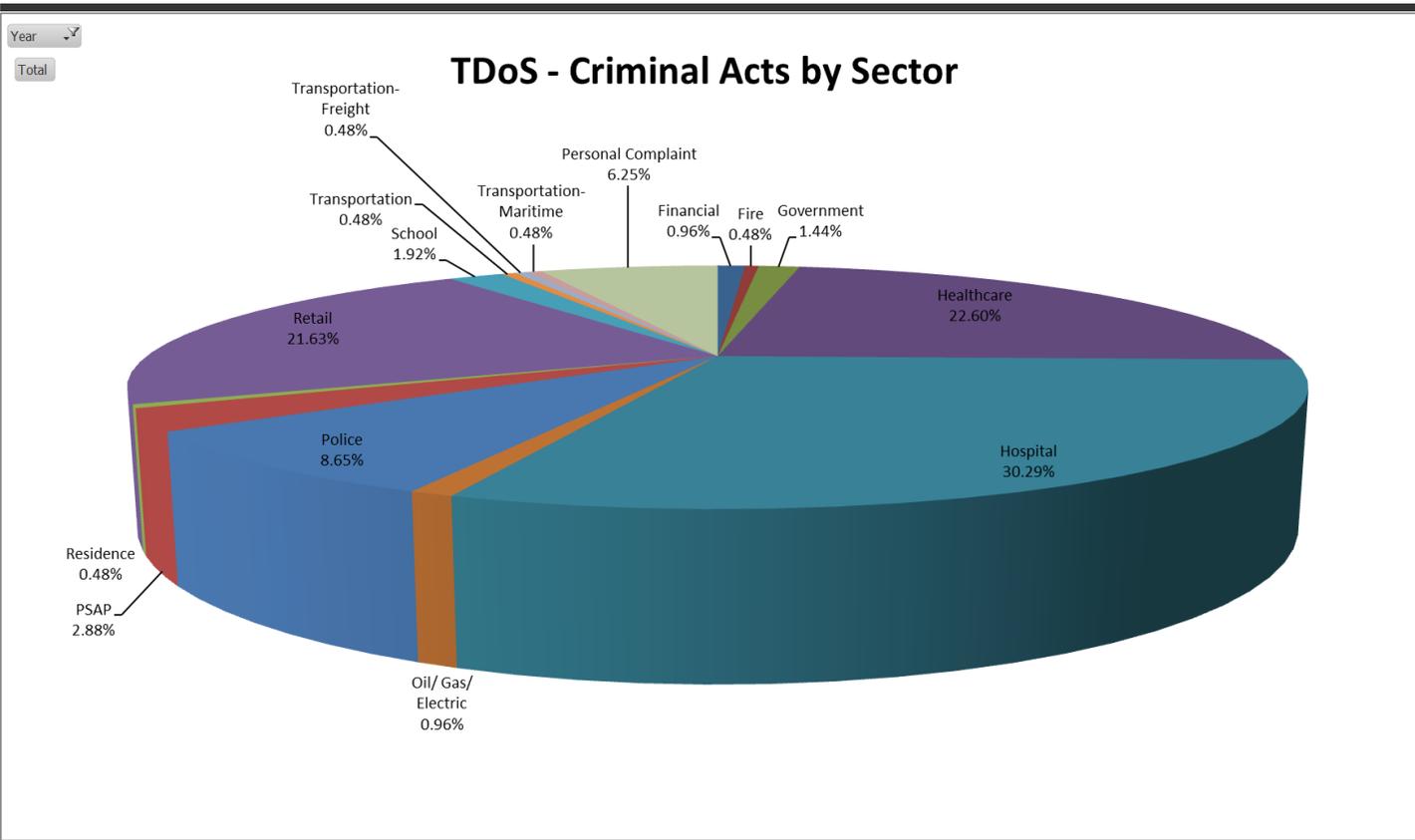
2011: TDoS – Criminal Acts by Sector



Sector	Total
Communications	1
Healthcare	9
Hospital	7
Oil/ Gas/ Electric	1
Police	5
PSAP	1
Retail	18
Security	1
Transportation-Freight	1
Personal Complaint	4
Grand Total	48



2012: TDoS – Criminal Acts by Sector



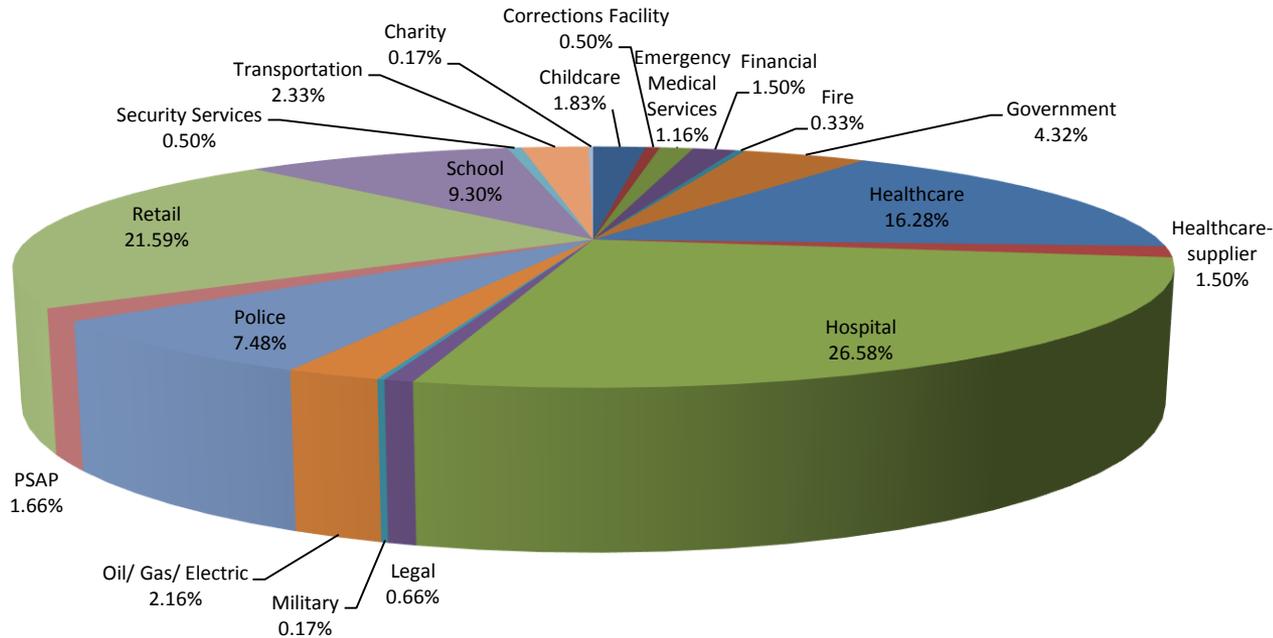
Sector	Total
Financial	2
Fire	1
Government	3
Healthcare	47
Hospital	63
Oil/ Gas/ Electric	2
Police	18
PSAP	6
Residence	1
Retail	45
School	4
Transportation	1
Transportation-Freight	1
Transportation-Maritime	1
Personal Complaint	13
Grand Total	208

433% Increase in Tracked TDoS Activity from 2011



2013: TDoS – Criminal Acts by Sector

TDoS - Criminal Acts by Sector



Sector	Total
Childcare	11
Corrections Facility	3
Emergency Medical Services	7
Financial	9
Fire	2
Government	26
Healthcare	98
Healthcare-supplier	9
Hospital	160
Legal	4
Military	1
Oil/ Gas/ Electric	13
Police	45
PSAP	10
Retail	130
School	56
Security Services	3
Transportation	14
Charity	1
Grand Total	602

289% Increase in Tracked TDoS Activity from 2012



2013: TDoS – Criminal Acts by Sector

2013 Summary of TDoS Attacks

Sum of 'Total'	Total
Business Type	
Redacted	5
Ambulance Service	1
Communications	5
Financial	4
Fire	3
Government	19
Healthcare	73
Healthcare-supplier	3
Hospital	122
Oil/ Gas/ Electric	14
Other	2
Police	35
PSAP	8
Public Transportation	2
Retail	128
School	41
Security	3
Transportation-Freight	6
(blank)	6
Transportation	1
Emergency Medical Services	4
Corrections Facility	1
Grand Total	486

Geographical Region Primary City, State	'Total'
Chesterfield, MO	18
Houston, TX	17
Chicago, IL	15
Bellwood, IL	14
Bone, NC	13
Guttman, MS	13
Lafayette, LA	13
Baltic, OH	12
Irving, TX	12
Los Angeles, CA	12
Moody, AL	12
Alameda, CA	11
Ann Arbor, MI	11
Ansonia, CT	10
Antioch, TN	10
Arlington Heights, IL	10
Crystal Lake, IL	10
Aurora, IN	9
Autauga Ville, AL	9
Belleville, MI	9
Crawfordsville, KY	9
Pine Bluff, AR	9
Addison, IL	8
Alexandria, IN	8
Amylin, OH	8
Birmingham, MI	8
Bon Weir, TX	8
Burlingame, CA	8
Beverly Shores, IN	7
Castaic, CA	7
Cleveland, NC	7
Dos Palos, CA	7
Lees Summit, MO	7
MacDonald, TX	7

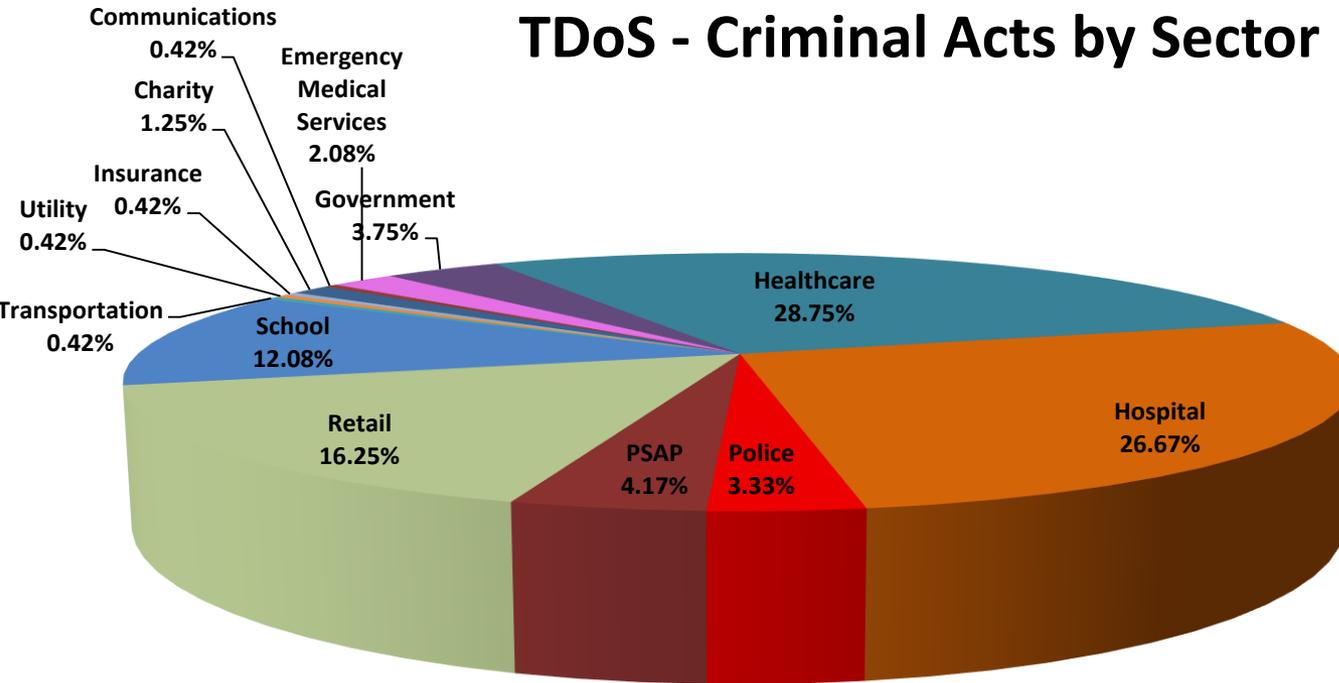
(U/FOUO) – Total of 178 Victims

Long List –
Names A-L



2014: TDoS – Criminal Acts by Sector

TDoS - Criminal Acts by Sector



Sector	Total
Charity	3
Communications	1
Emergency Medical Services	5
Government	9
Healthcare	69
Hospital	64
Police	8
PSAP	10
Retail	39
School	29
Transportation	1
Utility	1
Insurance	1
Grand Total	240



Some Examples of TDoS Attacks (2013)

- US Coast Guard – May. Service member's bank account had been compromised, causing loss of personally identifiable information (PII)
- Sheriff's Office – January-March, south central U.S. PSAP was attacked in extortion attempt purportedly based on an employee's default on a personal loan.
- State legislative office – January-March, south central U.S. state. Caller sought to speak to former employee claiming unpaid debts.

// UNCLASSIFIED – FOR OFFICIAL USE ONLY //



Homeland
Security

Office of Emergency Communications

TDoS: Answering Point Best Practices

Before an event:

- Discuss how to respond to a TDoS event with your service provider. These discussions might include both your telephone service providers (9-1-1 and Administrative phones - if separate providers) as well as your 9-1-1 equipment vendors.
- Ensure that the telecommunicators and their supervisors have access to the phone number and direct contact information for the service provider's personnel or division equipped to respond to a public safety TDoS.
- Discuss with your telephone system engineer or technician possible configuration changes to isolate critical phone lines (incoming 9-1-1 calls for service) from administrative and other lines, taking into account hunt-groups, busy or no-answer rollover to other lines ...



APCO Best Practices Guide, 3/2013

Copies of three “best practices” guides for PSAP’s are offered for your consideration. While one is Verizon’s, I believe you can customize it for your provider. Most TDoS concepts that apply to PSAPs will apply to critical infrastructure entities, too.



Homeland
Security

Office of Emergency Communications

TDoS: Answering Point Best Practices

During an event:

- Save the voice recording of suspects who may call before, during or after the TDoS
- Record all telephone numbers and account information (if caller demands payment).
 - Start and stop time of the event
 - Number of calls per hour (if known)
 - Phone numbers and other ANI/ALI of incoming calls
 - IP addresses, if applicable
 - Instructions for how to pay (account numbers, call back numbers, etc.)
- Attempt to separate the affected phone number from 9-1-1 and other critical trunks – work with your PBX or switch provider/administrator.



APCO Best Practices Guide, 3/2013



Homeland
Security

Office of Emergency Communications

TDoS: Answering Point Best Practices

After an event:

- File a complaint with the Internet Crime Complaint Center and National White Collar Crime Center (www.IC3.gov). Include the keywords **TDoS**, **PSAP**, and **Public Safety** in the description of the incident.
- File a report with your local PD or Sheriff's Office. IF the investigator is unsure how to proceed, the FBI, FCC, FTC (Federal Trade Commission) are all engaged in working on TDoS.
- Advise the investigator the CALEA (Communications Assistance for Law Enforcement Act) protocol can be invoked, enabling service providers to collect data on the originator of the call for law enforcement purposes.
- Consolidate call logs and IP logs; mark for long term retention.



APCO Best Practices Guide, 3/2013



Homeland
Security

Office of Emergency Communications

TDoS: Answering Point Best Practices

After an event:

- Share information about the incident (to the extent possible) with other 9-1-1 Centers/PSAPs and private call centers, such as emergency medical services (ambulance, air ambulance) dispatch points and similar agencies you work with on a daily basis.
- Notify the Iowa Intelligence Fusion Center:
(800) 308-5983 or e-mail at intel@dps.state.ia.us
- ❖ *Fusion Centers* play a critical role in rapid interstate sharing of these types of incidents. The discovery of TDoS attacks occurring was based on information sharing in the Southeast U.S. - Florida and Louisiana fusion centers were first to “connect the dots.”



TDoS: Answering Point Best Practices

After an event:

- The DHS NCCIC National Coordinating Center for Communications can also help facilitate information sharing with carriers and submission of information to FBI's Internet Crime Complaint Center.
24/7 Watch Desk (703) 235-5080 ncc@hq.dhs.gov
- Share information about the incident with other 9-1-1 Centers/PSAPs and private call centers, such as emergency medical services (ambulance, air ambulance) dispatch points and agencies you work with on a daily basis.



TDoS: Non-Service Initiated Wireless Phones

NSI Wireless Handsets: for the “Greater Good?”

- FCC 08-51 NOI regarding 911 Call-Forwarding Requirements and Carriers Blocking under review (reportedly close to rule making)
- It’s almost impossible to trace a low power, battery powered handset by mobile direction finding, making FCC Enforcement Bureau action very difficult
- Some filers in the open proceeding suggest 2% or fewer of their NSI 9-1-1 calls are valid (Tennessee ECB)



TDoS: Non-Service Initiated Wireless Phones

NSI Wireless Handsets: for the “Greater Good?”

- Carrier’s filings generally oppose being forced to block wireless 911 calls (liability concerns)
- Relationships with the carrier (through Iowa E-911 Council/TSI or your own PSAP) are usually BEST resource for assistance



TDoS: Non-Service Initiated Wireless Phones

- If persistent, notify law enforcement and your Iowa Intelligence Fusion Center. Situational awareness of the problem may not be apparent at the local, county, or even your state level.
- There are some innovative ideas being developed on a trial basis to help deal with the nuisance calls, but the solution is expensive. One filing in the FCC proceeding suggested a portal where individual PSAP's could block calls by an ANI entry. Would your county or board's attorney sign a liability release to give your center this capability?



TDoS: Non-Service Initiated Wireless Phones

- An FCC regulatory decision is probably our best hope. As long as carriers are *required* by the FCC to complete 911 calls from NSI equipment, blocking calls without a significant showing of need is a serious operational liability the carriers eschew.



Improving 9-1-1: Advising the FCC

911.gov | News

The Federal Communications Commission – one of the National 911 Program's Federal Partners in supporting optimal 911 services across the nation – has announced a request for membership nominations to a task force focused on optimal PSAP architecture.

This task force is being asked to consider several important issues, including:

- Optimal PSAP system and network configuration in terms of emergency communications efficiency, performance and operations functionality
- Cost projections for conversion to an annual operation of PSAPs that incorporate such optimal system design
- Comparative cost projections for annual maintenance of all existing PSAPs and NG911 upgrades
- Recommendations to ensure states use E911 funds for the intended purpose
- If states with diverted 911 funds should be ineligible to participate in certain FCC activities

Please consider submitting nominations to the FCC by the **November 7th** deadline and review the [FCC notice](#) for more detail.



Your Turn: NSI Wireless Phones



OEC Priority Telecommunications Services

Priority Services programs provide NS/EP and public safety users the ability to communicate on telecommunications networks during times of congestion.

- Government Emergency Telecommunications Service (GETS)
- Wireless Priority Service (WPS)
- Telecommunications Service Priority (TSP)



GETS and WPS Applications

GETS and WPS provide priority access to the landline and cellular networks when abnormal call volumes exist, providing enhanced call completion for critical NS/EP personnel.

GETS and WPS can be used to supplement public safety communications during times of network congestion:

- Contact off-duty personnel on their home/cell phones
- Communicate with response personnel that do not have radio access (e.g. Red Cross, volunteers, utility companies)
- Discuss sensitive information that may not be appropriate for radio broadcast
- Maintain communications with leadership
- Access to teleconferencing capabilities



GETS: Solution for Wireline Congestion

GETS provides priority access to the landline network when abnormal call volumes exist, providing enhanced call completion for critical NS/EP personnel.

- GETS has historically provided over 90% call completion rates
- For hurricanes Isaac, Irene, and Sandy over 99% of GETS calls were completed
- GETS can be used from virtually any *landline telephone* to provide priority for emergency calls
- GETS is available to approved users at no cost
- It provides priority queuing of calls over the landline network - not a separate system



GETS Overview

1. Dial GETS Access Number from any phone (1-710-627-4387)

2. Network routes call to a GETS Carrier. As you are prompted, enter your PIN then Destination Number

3. Network routes your call to the Destination Number



Use GETS whenever you hear a fast busy signal, "All circuits busy" announcement, or otherwise cannot complete your call.



WPS: Solution for Wireless Congestion

WPS provides priority voice access to the cellular network when abnormal call volumes exist, providing enhanced call completion for critical NS/EP personnel.

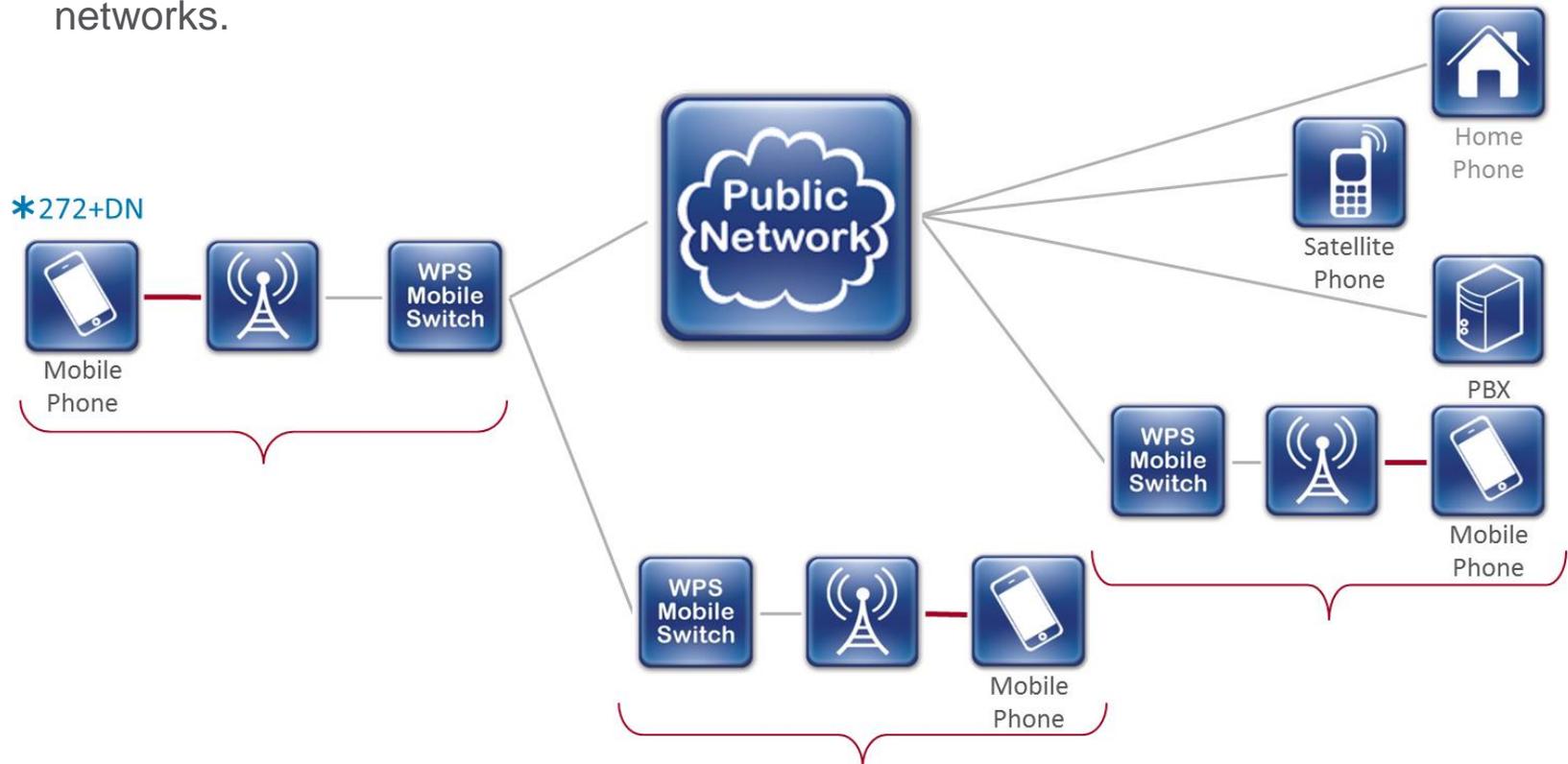
- WPS has historically provided over 90% call completion rates
- During Hurricane Sandy, over 98% of GETS calls were completed. During the Boston Marathon Bombing incident response, WPS was essential to complete calls in the incident area for *hours after the incident*.
- WPS is available on all the major cellular carriers and many regional cellular carriers
- WPS is an add-on feature and must be added to each applicable cell phone subscription; no special phones/equipment are required
- Calls must be placed through the subscribed phone to receive priority access to the network



WPS: Functional Diagram

1. WPS is an add-on feature subscribed on a per-cell phone basis – works with existing cell phones in WPS equipped networks.

2. To make a WPS call, enter *272 followed by the Destination Number then press SEND.



WPS addresses congestion in the wireless segment of the network – most importantly the local radio access channel.



TSP: Provisioning and Restoration

Provisioning



- TSP authorizes priority installation of new voice and data circuits
- Organizations must be registered with TSP before requesting priority installation

Restoration



- Organizations designate critical circuits to have priority repair and restoration if damaged.
- Circuits must be registered with TSP prior to requesting priority restoration



TSP Applications

TSP provides priority repair and installation of critical voice and data circuits

TSP provisioning and restoration is essential for:

- Repair/replacement of damaged circuits at EOCs, hospitals, PSAPs, power facilities, government headquarters, financial institutions, etc.
- Priority installation of new circuits when needed to support operations such as disaster response and recovery, inaugurations, and large scale national security events.



Homeland
Security

Office of Emergency Communications

Questions?

OEC

oece@oec.dhs.gov

WEB

www.dhs.gov/oec

www.publicsafetytools.info

Jim Lundsted

Office (573) 298-0484

Cell (202) 630-1177

James.Lundsted@hq.dhs.gov



Homeland
Security

Office of Emergency Communications



Homeland Security