



Telephony Denial of Services (TDOS) to Public Safety Communications Phone Service

Recommended Best Practices Checklist

Information continues to be received from multiple jurisdictions indicating the existence of ongoing attacks targeting the telephone systems of public sector entities. Over 200 such attacks have been identified to date. The perpetrators of the attack launched numerous phone calls against the target telephone network, tying up the system and preventing the agency from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service Attack.

As a result of a cooperative effort between Federal Authorities, public safety representatives, and commercial service providers, the following checklist has been developed to provide you with information that will assist in the development of a continuity of operations plan for your agency.

1. Before an event:

- a. 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.
- b. Ensure that the Public Safety 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.
- c. 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, rollover to other PSAPs, etc. Prevent an overload of non-critical lines from rolling-over to lines answered by 9-1-1 call-takers
- d. Remind employees of their obligations to protect personally identifying information, and how to protect themselves from identity theft (for example, see <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>). Additionally, if an attack were to occur at your agency reassure the targeted employee that they are not responsible for the attack. They and the center are merely victims of a highly sophisticated criminal enterprise.

2. During the event:

- a. Save the voice recording of suspects who may call before, during or after the TDoS events.
- b. Record all phone numbers and account information, if the caller is demanding payment(s):
 - i. Start and stop times of the events
 - ii. number of calls per hour or per day
 - iii. phone numbers and other ANI/ALI information of the incoming calls
 - iv. IP addresses if applicable
 - v. Any instructions for how to pay, such as account number, call-back phone number etc.
- c. Retain all call logs and IP Logs
- d. Attempt to separate the affected phone number from 9-1-1 and other critical trunks – work with your PBX provider/maintainer.

3. After the event:

- a. File a complaint with the Internet Crime Complaint Center www.IC3.gov - co-sponsored by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). Include the keywords **TDoS, PSAP, and Public Safety** in the description of the incident
- b. File a report with your local police department or sheriff's office.
 - i. If the investigator is unsure of how to proceed there are resources available to assist. The FBI, FCC (Federal Communications Commission) and FTC (Federal Trade Commission) are all engaged in this process, and DHS-NCC- NCCIC (Department of Homeland Security - National Coordinating Center for Communications - National Cybersecurity and Communications Integration Center) can help coordinate information.
 - ii. Advise them that the CALEA (Communications Assistance for Law Enforcement Act) protocol can be invoked, enabling service providers to collect data on the originator of the call and provide it to law enforcement resources.
- c. Consolidate call logs and IP logs; mark for long-term retention.

9-1-1 Centers / PSAPs should also make efforts to share this information with other public safety facilities with which they interact including: private ambulance service dispatch centers, hospitals, air ambulance dispatch centers etc.