To: Industry and Government Partners, Routine

The Department of Homeland Security (DHS) NCCIC - National Coordinating Center for Communications – the DHS-Office of Emergency Communications, DHS - Office of Infrastructure Protection, Federal Communications Commission, the National Cyber and Forensics Training Alliance, the FBI-National Cyber Investigative Joint Task Force working in coordination with the Association of Public Safety Communications Officials (APCO) International, the National Emergency Numbers Association (NENA), Louisiana Fusion Center, Mansfield Police Department and telecommunications service providers to identify and mitigate the effects of a criminal Telephony Denial of Service (TDoS) against public safety communications, hospitals and ambulance services. This is for immediate dissemination to public safety answering points (PSAPs) and emergency communications centers and personnel.

Background: Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line), The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occurred targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications.

Scheme: These recent TDoS attacks are part of an extortion scheme. This scheme starts with a phone call to an organization from an individual claiming to represent a collections company for payday loans. The caller usually has a strong accent of some sort and asks to speak with a current or former employee concerning an outstanding debt. Failing to get payment from an individual or organization, the perpetrator launches a TDoS attack. The organization will be inundated with a continuous stream of calls for an unspecified, but lengthy period of time. The attack can prevent both incoming and/or outgoing calls from being completed. It is speculated that government offices/emergency services are being “targeted” because of the necessity of functional phone lines.

What we know:

- The attacks resulted in enough volume to cause a roll over to the alternate facility.
- The attacks last for intermittent time periods over several hours. They may stop for several hours, then resume. Once attacked, the attacks can start randomly over weeks or months.
- The attacks followed a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did.
- There have been approximately 600 related attacks against a variety of victims, including approximately 200 against public safety reported and being investigated

What we need from victims:

- Additional insight into the scope and impact of the event- specifically how many communications centers have been attacked is critical to identifying the true scope of this occurrence.
- In order to ensure situational awareness with our members and member agencies, it is critical that this information be disseminated to emergency communications centers, PSAP's, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operations.

Recommend the following:

- Targeted organizations should not pay the blackmail.
- Report all attacks to the FBI by logging onto the website www.ic3.gov
    - Ensure in the title of the report you use the keyword TDoS
    - Ensure that you identify yourself as a PSAP or Public Safety organization capture as much details as possible
        - Calls logs from "collection" call and TDoS
            - § Time, date, originating phone number, traffic characteristics
        - call back number to the "collections" company or requesting organization
            - · method of payment and account number where "collection" company requests debt to be paid
            - · ANY information you can obtain about the caller, or his/her organization will be of tremendous assistance in this investigation and in preventing further attacks.
- Contact your telephone service provider; they may be able to assist by blocking portions of the attack.
- Should you have any questions please contact the National Coordinating Center for Communications at NCC@hq.dhs.gov or 703-235-5080