(U) HANDLING THREATS TO PRIVATE CITIZENS AND LOCATIONS NAMED ONLINE BY VIOLENT EXTREMISTS

DUTY-TO-WARN RECOMMENDATIONS FOR THE LOCAL LAW ENFORCEMENT AGENCY

(U//FOUO) The fusion center has no information to indicate specific or credible threats to people whose names have been published online by violent extremists. You are being provided this advisory to assist your agency in responding to queries from members of the public or other concerned parties. This information, which often includes personally identifiable information (PII) obtained maliciously via the Internet, most likely represents aspirational threats. Its primary purpose is likely to heighten anxiety and a sense of vulnerability. It is unlikely that violent extremist-inspired individuals in the United States will target people identified online, but this cannot be ruled out entirely.

Issued 09/2017

(U) RECOMMENDATIONS FOR THE PRIMARY
LAW ENFORCEMENT AGENCY

(U//FOUO) When the FBI and/or the fusion center notifies you that a citizen in your jurisdiction has been threatened or an address in your jurisdiction has been listed in an online threat by a member or purported member of a violent extremist group, there are several ways your agency can assist, including but not limited to the following:

- Perform database checks of your local records management system and computer-aided dispatch (CAD) system for records or calls for service to the subject of the threat or address listed, and provide results to the FBI and the fusion center.
- Enter the address into the CAD system for future dispatch and patrol situational awareness related to the threat.
- Notify the FBI and the fusion center of any future suspicious activity reports (SARs) or calls for service regarding the victim of the threat or listed addresses associated with the threat.
- If your agency intends to make unilateral contact with a named victim and/or address, the FBI and the fusion center request that you coordinate with them first to avoid duplication of effort.
- If your agency decides to make unilateral contact with the victim, use the following as a guide to ensure consistency regarding unilateral notifications:
  - Your name and/or address was posted as part of a large list of Americans by an individual/group advocating that violent action be taken against people and addresses on the list.
  - These lists contain a large number of names and addresses, many of which were obtained by an individual or group posting them through open-source research using websites and online mediums that likely contain your personal information.
  - Although the individual or group posting the threat advocates violence, that individual or group may not have the capability to harm you. However, we are notifying you of the threat out of an abundance of caution.
  - Your local law enforcement agency is here today to let you know that we have notified our dispatch and patrol personnel of this threat for your safety and protection.
  - In an abundance of caution, we urge you to report any suspicious activity by calling 9-1-1 or the appropriate emergency number of your local law enforcement agency for immediate response. The agency will notify the FBI Joint Terrorism Task Force and fusion center of any suspicious activity reports.
  - Consider referring victims to identitytheft.gov if their PII was compromised.
  - If a victim's work-related information is disclosed, recommend that the victim notify his or her employer in the event that contact is made via the victim's work account.
- Law enforcement agencies should use best cyber hygiene practices when reviewing or downloading any potentially untrusted source lists that identify victims, since the documents may contain links to malicious software.

Additional information on how to deter data compromises is available via the ***Understanding Digital Footprints: Steps to Protect Personal Information*** resource: https://it.ojp.gov/GIST/1191/File/Understanding%20Digital%20Footprints-09-2016.pdf.

(U) BEST PRACTICES TO HELP DETER DATA COMPROMISES

- Limit the amount of personal information you post online and on public-facing online platforms.
- Be wary of unsolicited contacts on social media requesting personal information.
- Evaluate your security or privacy settings and limit access to your information.
- Use strong, complex, and unique passwords on all accounts. Enable two-factor authentication when possible.
- Check privacy policies and limit options for individuals viewing your social media account, as well as accounts associated with family members.
- Regularly monitor credit reports and associated financial information for any potential compromise.
- Understand what personal information may be available as public record.
- Report suspicious activity to mitigate potential targeting.
- Ensure that all of your devices have antivirus software and are continually updated.