INFORMATION ASSURANCE DIRECTORATE

"INFORMATION ASSURANCE LEADERSHIP FOR THE NATION"

(U) INFORMATION ASSURANCE **Date: 24 AUG 2012**
(U) ADVISORY NO. IAA-008-2012

SUBJECT: (U//FOUO) Mitigations Guidance for Distributed Denial of Service Attacks

1. (U//FOUO) Adversary actors in cyberspace continue to demonstrate the interest in and ability to execute Distributed Denial of Service (DDoS) attacks against the United States. The need to offer Internet services in support of mission requirements inherently exposes these services to malicious traffic and the potential for DDoS attack. Proactive preparation to ensure network resilience in the event of a DDoS event is essential. Reactive measures are feasible, but are often too slow to respond to the dynamic nature of today's threat.

2. (U) **Proactive DDoS Protections**

   a. (U) Establish connections with multiple Internet Service Providers (ISPs) for redundancy.
   b. (U) Ensure Service Level Agreements with ISPs contain provisions for DDoS prevention (eg: through IP address rotation).
   c. (U) Design network with redundant systems and sufficient excess capacity.
   d. (U) Conduct rate-limiting of traffic at the network perimeter.

      (U) **Note:** Quality of Service for Legitimate Traffic may also be adversely affected.

   e. (U) Creation of backup, remote-site network infrastructure utilizing multiple addressing schemes
   f. (U) Content Delivery Network (CDN) providers which host geographically or logically separated services can limit the impact of DDoS attacks.

3. **(U) Reactive DDoS Protections:**

   a. (U) Execute Internet Service Provider address rotation.
   b. (U) Blocking of source IP addresses generating DDoS traffic at enterprise boundary or within ISP infrastructure

      (U) Note: Adversary capabilities will make blocking of individual addresses (or even blocks of addresses) very difficult to implement.

   c. (U) Acquire increased bandwidth capability from ISP.

4. (U//FOUO) DDoS attacks are often used as a diversion for other more targeted attacks. Victims of DDoS attacks should conduct thorough reviews of their network infrastructure following an attack to ensure no additional malicious activity was conducted during or subsequent to a DDoS.

5. (U//FOUO) Questions concerning this Advisory should be directed to the NSA Information Assurance Customer Advocate Office at 410-854-4790.