**Service Outage Prevention and Mitigation**

*Submitted By: SOS (Service Outage Support) sub team*

*Accepted: 09/13/2022*

*Version: 1*

**Version History**

This BP (Best Practice) was created by the SOS (Service Outage Support) sub team of the NPIF (Number Portability Industry Forum) in response to PIM 142 - DDoS (Dedicated Denial of Service) attacks.

**Background**

This BP was created to address concerns about the use of number portability to reroute telephone numbers in situations where a Service Provider is experiencing call completion issues related to network attacks such as DDoS.

PIM 142 - DDoS Attacks was created and accepted by the NPIF to discuss this issue. After discussion at the 02/07/2022 NPIF a new sub-team, SOS was created to discuss/address the issue. After several meetings, a consensus was reached by the SOS to refer the issue to ATIS NGIIF (Next Generation Interconnection Interoperability Forum) to seek assistance in determining if a solution other than utilizing number portability existed or could be created. The NGIIF referred the request to the ATIS NRSC who discussed the issue and provided the spreadsheet embedded below (Best Practices from NGIIF 071122) in the Prevention section.

**Documentation Referenced:**

* [PIM 142 - DDoS Attack](https://workinggroup.numberportability.com/documents/8258/PIM_142_-_DDoS_Attack_1.docx)
* [BP 069 - Large Port Notification](https://workinggroup.numberportability.com/documents/6584/0069_Large_Port_Notifications_v3.docx)
* [FRS (Functional Requirements Specification)](https://numberportability.com/documents/8198/FRS_R5.1_02-06-2022.docx)

**Decisions/Recommendations**

Service Providers are susceptible to IP network attacks such as DDoS. Industry Best Practices (NGIIF reference) should be implemented, and it is strongly recommended that any/all Industry Best Practices should be utilized in the prevention of DDoS attacks. Use of number portability as a solution should be a last resort In the mitigation of a DDoS attack. The current number portability ecosystem (Local systems, Network components, NPAC) is not equipped to support the porting volumes and short timeframes required to quickly remediate outages caused by these types of attacks

**Prevention**

DDoS and other attacks that impact networks and specifically telephone call completion evolve rapidly and therefore cannot always be prevented. However, to avoid being impacted by a DDoS or other attack, Service Providers and their vendors should follow Industry Security Best Practices such as those listed in the embedded spreadsheet (Best Practices from NGIIF 071122



In addition, the NGIIF provided the following guidance in the prevention of DDoS attacks:

*NRSC pointed NGIIF to online resources outlining similar recommendations, including the New Jersey Cybersecurity & Communications Integration Cell’s (JCCIC) DDOS Attack Types and Mitigation Strategies webpage (*[*https://www.cyber.nj.gov/this-is-security/ddos-attack-types-and-mitigation-strategies*](https://nam10.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cyber.nj.gov%2Fthis-is-security%2Fddos-attack-types-and-mitigation-strategies&data=05%7C01%7Cmdoherty%40iconectiv.com%7Ce9c78fcc54994f99c87e08da7a191cf1%7C69c8e407b674422eb87b0e5394e0005e%7C1%7C0%7C637956545520135391%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=xbcnV%2B%2FPSPTf9WXJbRbeVsKawvSs60UpqNkG4liQ2Hw%3D&reserved=0)*).*

*Additionally, NGIIF members worked with internal experts to understand what service reinstatement could look like.  One provider mentioned that their network engineering team concurred with NRSC’s findings that when dealing with a DOS attack, providers must focus on prevention and mitigation efforts.*

*This provider listed four ways to help with DOS prevention:*

1. *Direct Connections with Customers and Peering Partners (Carriers)*
   * 1. *A direct connection will allow traffic to bypass the public internet, which is typically the source of DOS attacks and thus offer additional security due to its private nature.*
     2. *The internet cannot always be avoided and therefore the hardware used to build the network will still need additional prevention methods (see below).*
2. *Robust Routing Hardware*
   * 1. *Service providers should deploy modern routing hardware that is carrier grade.*
3. *Increased Capacity*
   * 1. *Transit and backbone connections between Points of Presence (PoP) should have increased capacity that can help absorb leakage from a DOS attack after proper mitigation.*
   1. *DOS Mitigation Services*
4. *Mitigation services should be deployed to an upstream Network Service Provider (NSP) or DOS provider to filter and block DOS attacks from reaching the Service Provider’s network.*
5. *Legit traffic should be passed after the DOS mitigation service scrubbing*

**Remediation after attack has been propagated:**

When service outages occur and the only available remediation method is to utilize number porting to change the LRN to route numbers to another network, the following Best Practices should be followed:

* Affected Service Providers should identify the highest priority customers to port, e.g., law enforcement, hospitals, etc.
* Follow Best Practice 069 - Large Port Notification by working with the NPAC HelpDesk.
* Porting should be done in a manner that does not impact the entire ecosystem in accordance with the FRS -Definition of Rate Requirements and Assumptions (R6-28.1, R6-28.2, RR6-107, RR6-108, RR6-109, AR6-3, AR6.4, AR6-5, AR6-7)
* Perform necessary diligence to avoid the creation of redundant/duplicate records which can occur when SVs are created in pool blocks (especially with larger porting activities) with identical information.