COMMUNICATIONS SECTOR COORDINATING COUNCIL
COMMENTS FOR
SECURE INTER-DOMAIN ROUTING
ROUTE HIJACKS

The following comments are provided on behalf of the Communications Sector Coordinating Council (CSCC) to the National Cybersecurity Center of Excellence (NCCOE) on the recently released draft project entitled "Secure Inter-Domain Routing: Route Hijacks."

The CSCC was established in 2005 to help coordinate initiatives to: (1) improve the physical and cyber security of Communications Sector assets; (2) ease the flow of information within the sector, across sectors and with designated federal agencies; and (3) address issues related to response and recovery following an incident or event. The CSCC's 40 members broadly represent the sector and include: cable, commercial and public broadcasters; information service providers; satellite, undersea cable, and utility telecom providers; service integrators; equipment vendors; and wireless and wireline owners and operators and their respective trade associations. Collectively the CSCC represents more than 33 U.S. companies and several trade associations covering hundreds more companies in our industry. The Communications Sector also was identified by Presidential Policy Directive 21 (PPD-21) as one of 16 Critical Infrastructure and Key Resource (CI/KR) sectors and has a long history of cooperation within its membership and with the Federal Government with respect to national security and emergency preparedness (NS/EP).

In these comments, we are providing feedback on the project description provided by the NCCOE regarding secure inter-domain routing. As noted on the NCCOE website, the National Institute of Standards and Technology (NIST) has begun the development of a Special Publication (SP 800-189) that is intended to provide security recommendations for the use of Inter-Domain protocols and routing technologies with an objective to protect the integrity of Internet traffic exchange. NCCOE's project description also discusses the concept of implementing BGP route validation (ROV) based upon Resource Public Key Infrastructure (RPKI) that in theory can mitigate accidental hijacks and malicious attacks associated with route hijacking. Finally, the NCCOE notes that wide-scale deployment of RPKI-based ROV could significantly enhance the overall security and robustness of the Internet.

The CSCC applauds NIST for initiating a project to address the lingering concerns with the functionality, performance, availability, scalability, and policy implications associated with inter-domain routing. Inter-domain routing is an issue that the Communications Sector has worked on for many years. The Communications Sector participated in two separate Federal Communications Commission (FCC) Communications Security Reliability and Interoperability Council (CSRIC) working groups (CSRIC III

Working Groups 4 and 6) that produced reports on network security best practices, including Border Gateway Protocol (BGP) Security best practices and secure inter-domain routing.[1]

The Working Group 6 report should be of particular interest to the NCCOE, as the Working Group was tasked with reviewing Secure BGP Deployment, including RPKI. The CSRIC report focuses on "providing high-level guidance concerning participation in RPKI, and a high-level analysis of risks of RPKI." The Working Group proceeded to provide several key recommendations:

First, that there be a concerted effort to develop accurate records about Internet number resource holders. Nearly all techniques for improving the security of inter-domain routing rely on authoritative, accurate and timely information about which Autonomous Systems (AS) are authorized to originate routes for each Internet Protocol (IP) address block. Part of this recommendation suggests that Internet number resource holders should start to use RPKI to generate certificates and route original authorizations (ROAs). This is critical to the success of any route validation or PKI based security regime. To perform validation there must be an accurate and secure source to validate against. In our view, this source does not exist yet.

Second, the Working Group recommended the cautious, staged deployment of RPKI origin validation (ROV). The report recommends that AS operators should follow a cautious and staged deployment of RPKI, starting by using RPKI data in an out-of-band fashion as one of several ingredients for detecting suspicious routes and constructing their route filters. Any future fully-automated use of RPKI data in filtering "invalid" routes should come only after AS operators are highly confident in the reliability and timeliness of the RPKI data and full understand the impacts on network performance.

Third, the Working Group recommended that steps be taken to mitigate risks inherent to RPKI. There is risk that even an RPKI system could be exploited, such as by attackers embedding false routes into the RPKI infrastructure itself. There remains risk that RPKI itself could be exploited. Thus, the NCCoE project should include the development of guidelines for the structure of the RPKI hierarchy and policies/rules for participating in the RPKI to ensure that it is technically infeasible that the RPKI can be exploited. Further, to address this concern, the CSRIC Working Group recommended that it should be possible to easily correlate RPKI data with the identities of resource holders that are decoupled from RPKI records and that organizations responsible for operating RPKI databases and managing certificates make available tools to detect possible configuration errors and expiring certificates, as well as to flag suspicious changes that may stem from abusive manipulation of the data.

In the Communications Sector's view, many of these issues remain unresolved. Thus, although we appreciate the NCCOE initiating a project focused on RPKI validation we are concerned that the description as written glosses over several significant factors that must be considered as part of this work, many of which are reflected in the recommendations described above.

---

[1] CSRIC III developed two reports. The first was in Working Group #4 on Network Security Best Practices, including a section on BGP Security Best Practices. The second was in Working Group #6 and addressed Secure BGP Deployment, including the specific topic of ROV. The reports are available at the following links:
WG-4 - https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf
WG-6 - https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf

A better approach would be for the NCCOE to shift to conducting a Proof-Of-Concept of Secure Inter-Domain Routing including all aspects of the technology (BGP, RPKI, and BGPSec). The Proof of Concept could test the incremental steps required to get to a full deployment of Secure Inter-Domain Routing from today's deployments. Simplistically focusing solely on BGP validation misses all that is required to fully address the concerns with deploying Secure Inter-Domain Routing. BGP Route Validation addresses route hijacks, but that is only one vulnerability of BGP. Further, the project needs to account for the impact of RPKI in a variety of areas impacting network performance such as the impact of RPKI on processing time and latency; availability including both up time and recovery time; availability including the number of routes, number of ASNs, number of certificates in repository; and how many COI participants are needed and of what scale.

The proof of concept should then address and report on key concerns, such as the following:

- Complexities involved with configuring and running a certificate authority.
- Management of certificates, error cases for when certificates are not managed properly, such as failing to issue a certificate in a timely manner or issuing a new Route Origin Authorization (ROA) for an IP address block and invalidating its IP sub blocks.
- Action to take for invalid routes and unknown origins.
- Dealing with the use cases of deliberate manipulations of routes by third parties, such as the revocation of a certificate for an IP address block, and how this may compromise the reachability to/from those IP addresses.
- Commercial readiness of the technology and tools.
- Tools for debugging SIDR. Debugging BGP issues is already complicated, so it will be important to understand the readiness of the tools.

In closing, we appreciate the opportunity to submit comments and commend the NCCOE for its work to date. We urge the NCCOE to take these factors into consideration as it finalizes its project description and the Communications Sector looks forward to participating in the Community of Interest that is forming around this project.

Sincerely,

Robert Mayer
Chair, Communications Sector Coordinating Council