		Authors' responses to comments received on the 2nd Public Draft of NIST SP 800-189: "Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation" (publication date: October 2019). Changes based on these comments/responses are incorporated in the final publication of NIST SP 800-189 (published December 2019). (Note: Comments set #s here do not correspond with the same for the initial public draft.)	
		Note: SR# = Security Recommendation #	
Lines:	**SR#**	**Comments**	**Authors' response**
		Comments set #1	
		This publication is a phenomenal reference, providing a clear set of operationally relevant guidance and commentary.	Thank you for the compliments. Thank you for your diligent review/comments on the initial public draft.
		Comments set #2	
		This is an impressive effort!	Thank you.
		Comments set #3	
		Really, really nice to see that NIST pays attention. Thanks so very much for contributing to this effort. [We] think the document is a lot better than it was going in.	It was our pleasure to work with you. Thank you for your thorough review/comments on the initial public draft.
		Comments set #4	
		Excellent document.	Thank you.
		Have you considered making RFC 8212 (https://tools.ietf.org/html/rfc8212) "Default External BGP (EBGP) Route Propagation Behavior without Policies" a recommendation? I'm not aware of any vendor where default deny is implemented, but in some cases this can be done via commit-time scripts.	In the revised document, we have included the reference (RFC 8212) and a summary of the recommendations therein. Please see newly added Section 4.11.

		Note: SR# = Security Recommendation #	
Lines:	**SR#**	**Comments**	**Authors' response**
		Comments set #5	
		I have read the second draft of "Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation" and found it to be a comprehensive introduction into the subject of interdomain routing, giving good guidance and recommendations.	Good to hear that!
		Section 3.1: The main example in this section is Mirai. As you mentioned correctly, this particular attack did not use spoofed addresses. Since this paragraph is all about spoofing, there might be better examples.	We've now included new references [Arbor] [Arbor2] as primary references.
		Section 3.1: It is not clearly stated that IP spoofing is a necessary requirement for reflection attacks. This should be added.	You are actually referring to Section 3.2 here. Yes, we've added that IP spoofing is a necessary part of it.
485		Line 485: I do think that [TA14-017A] is a better pointer regarding amplification factors than [ISOC].	We've followed your suggestion and show [TA14-017A] and [ISOC] as the references, in that order.
1158-		Lines 1158ff: This paragraph might need some work. The text seems unfinished. The description/explanation of the example in figure 11 is less detailed than the description of the examples before although it is more complex. "DDoS Mitigation" has not been mentioned in this section before. There should either be more context and explanation or the example should be removed. I do not think that this example is necessary as there is currently no recommendation for EFP-uRPF.	Good observations. We've taken your suggestions into account and have carefully revised the paragraph. This is the last paragraph of Section 5.1.6.
		Comments set #6	

		Note: SR# = Security Recommendation #	
Lines:	**SR#**	**Comments**	**Authors' response**
486		I see on line 486 it states "The attacker typically makes use of a botnet consisting of many compromised devices...". This is not the case. The attackers are using an internet connection (normally just one) that allows spoofed traffic to be sent out. Normally this is a hosting company that either is incompetent and doesn't perform source address validation or they intentionally don't perform the source address validation. I would also suggest updating Figure 3 to reflect this.	We have made the changes you suggest in the revised document. The text has been updated in Section 3.2 and also Figure 3 has been revised to reflect your suggestions.
1351	59	Line 1351 states "An ISP should perform rate limiting of UDP fragment traffic at edge routers facing customers and lateral peers." I would specify "non-initial UDP fragments". This can also be specified as UDP packets where the fragment offset is greater than 0. These are the packets that do not have the L4 information in them.	We've updated SR #59 and the text in the paragraph preceding it per your suggestion.
		Comments set #7	
	35	Security recommendation 35: why only filter customer sessions with ROA data? Shouldn't filtering take place on all EBGP sessions?	We have now added a footnote to SR #35 that explains: "It is generally not feasible to apply this on peer interfaces because it is not possible to accurately know a peer's customer cone. Of course, BGP-OV (see Section 4.3) for detecting invalid prefix announcements is applied on all interfaces."
		Currently the draft only links to the RIPE validator; shouldn't links be included to NLnet Labs and Cloudflare OctoRPKI for example?	We have now included references to Routinator (NLNetLabs), OctoRPKI (Cloudeflare) and FORT also in Section 4.2.

		Note: SR# = Security Recommendation #	
Lines:	**SR#**	**Comments**	**Authors' response**
	51	Security recommendation 51: why only “smaller ISPs”?	We have now changed it to "ISPs" instead of "Smaller ISPs" in SR #51, but we have added a foot note to the SR that says, "Security Recommendation 51 is possibly more applicable to smaller ISPs that have accurate visibility of their customer cone. Larger ISPs tend not to have such visibility."
		Comments set #8	
		Consider mentioning the DHS supported project on open source measurement technology and service to allow anyone to test their SAV standards compliance: https://www.caida.org/projects/spoofer/	Thank you for pointing that out. In the revised document, we briefly describe the Spoofer project in Section 5 and have included two references (pointers) to the details of the work.
		Comments set #9	
		We appreciate NIST’s efforts to address concerns raised in our comments on the first draft of SP 800-189 (“First Public Draft”). Specifically, we are pleased to see NIST added a reference to the FCC’s Communications Security, Reliability, and Interoperability Council (“CSRIC”) Working Group recent report Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols published in March 2019 (“2019 CSRIC Report”). The Second Public Draft also helpfully bolsters references to international standards bodies and other industry-led work. [Our organization] also appreciates the edits to begin to clarify the voluntary nature of SP 800-189.	Thanks for these observations and your appreciation for our efforts. We are grateful also for your feedback on the initial public draft.

		Note: SR# = Security Recommendation #	
Lines:	**SR#**	**Comments**	**Authors' response**
		While NIST added a reference to the 2019 CSRIC Report in the Second Public Draft, SP 800-189 could be improved by further harmonization with that report. NIST recognizes the “significant commonality in terms of objectives for routing security and DDoS mitigation between [NIST’s work and CSRIC’s work].” NIST notes that SP 800-189 “addresses many of the same concerns regarding BGP vulnerabilities and DoS/DDoS attacks as highlighted in [CSRIC4-WG6] but goes into greater technical depth in describing standards-based and commercially available security mechanisms and providing specific security recommendations.”	We had a typo: we meant [CSRIC6-WG3] , not [CSRIC4-WG6]. Thanks for helping catch this mistake. Our response continues in the cell directly below.
		[Continued from above] NIST should be sure to refer to and harmonize with CSRIC’s most recent work in the 2019 CSRIC Report; the current discussion of the relationship between SP 800-189 and CSRIC references past CSRIC work. Additionally, continued close collaboration between the CSRIC and NIST efforts will help to reduce confusion and promote adoption of best practices. Because NIST is “committed to maintaining coordination with other interested groups that have shared interest in promoting security practices related to Internet routing, and ensuring that [its] document is in alignment with other efforts such as MANRS and the CSRIC report,” [our organization] would be happy to continue to work together.	We had a typo in the sentence that you quoted from our document. Sorry about that. We meant [CSRIC6-WG3] (not [CSRIC4-WG6]). So, we meant to refer to the same document that you call 2019 CSRIC Report. So yes, we feel we are good with regard to the alignment with 2019 CSRIC Report. And yes, we will plan to continue close collaboration with CSRIC. We'll certainly keep your suggestions in mind going forward. NIST SP 800-189 is expected to be updated in the future at times when appropriate. So, we welcome your offer to work together on an ongoing basis.

		Note: SR# = Security Recommendation #	
Lines:	**SR#**	**Comments**	**Authors' response**
		In our comments on the First Public Draft, we noted that the 2019 CSRIC Report highlights a University of Pennsylvania paper, Lowering Legal Barriers to RPKI Adoption, that discusses “legal barriers that may be hindering RPKI adoption in North America.” NIST “has been actively involved in fostering and facilitating support for the University of Pennsylvania work,” so it should explicitly discuss the January 2019 paper.	Thanks for pointing out our omission of the paper you mention. We were previously referencing only the NANOG presentation. We do now cite and discuss the January 2019 paper also in the revised document (at the top of Section 4 and in Section 4.2).
		It is important that NIST underscore the voluntary nature of SP 800-189, which is the hallmark of NIST’s most effective and widely adopted work [NIST's Cybersecurity Framework document]. While the Second Public Draft states that it “may be used by nongovernmental organizations on a voluntary basis” and “may also be useful for enterprise and transit network operators and equipment vendors in general,” NIST should ensure that it will not be seen as binding on industry.	The non-binding and voluntary nature of the document for nongovernmental organizations is clearly stated in the document. See additional response in the cell below.
		[Continued from above] NIST and [our organization] agree that SP 800-189 is voluntary for the private sector; NIST’s Summary of Comments and Responses confirms that “[n]othing elsewhere in the Draft is intended to imply otherwise.” To make clear its intent, NIST should reconsider how it uses words like “should,” especially in conjunction with recommendations that are relevant beyond the government and its contractors. We agree that “should” is better than “must,” but even “should” carries substantial weight in a document like this.	The use of "should" is appropriate for the primary audience which includes information security officers and managers of federal enterprise networks. See additional response in the cell below.

		Note: SR# = Security Recommendation #	
Lines:	**SR#**	**Comments**	**Authors' response**
		[Continued from above] Where appropriate, NIST might consider substituting “could” or “may” instead of “should,” or using language such as “should consider.” In a similar vein, some recommendations are worded broadly, making it appear to include all private sector parties: e.g., “All internet number resources (e.g., address blocks and AS numbers) should be covered by an appropriate registration services agreement with an RIR, and all point-of-contact (POC) information should be up to date.” The use of “all” suggests universal application, beyond government and contractor uses. NIST should disclaim any binding application of its recommendations, and consider how individual examples can be adjusted to be less prescriptive.	We feel that weakening the security recommendations with language such as "could" or "may" or "could consider" is not desirable for the primary audience (information security officers and managers of federal enterprise networks). For the private sector parties, the document clearly states, "This publication may be used by nongovernmental organizations on a voluntary basis." It is nice to see that companies such as AT&T, Telia, Cloudflare, AMS-IX, etc. are providing major leadership in adoption and deployment of RPKI and BGP-OV. There is a new study titled, "RPKI is Coming of Age ..." https://dl.acm.org/citation.cfm?id=3355596 .
		SP 800-189 promises to be a helpful contribution to “the security and robustness of interdomain traffic exchange.” The edits suggested above—along with NIST’s ongoing commitment to harmonize the various efforts, including the 2019 CSRIC Report and any future work that CSRIC engages in—will ensure that the document continues to evolve to address complex interdomain traffic exchange security issues.	Yes, thank you. Your suggested edits have been very helpful.