

**From:** [REDACTED]@cisecurity.org]  
**Sent:** 6/17/2020 12:58:15 PM  
**To:** [REDACTED]@twitter.com]  
**CC:** [REDACTED]@twitter.com]; [REDACTED]@cisa.dhs.gov]; [REDACTED]  
[REDACTED]@cisa.dhs.gov]; [REDACTED]@cisa.dhs.gov]; [REDACTED]  
[REDACTED]@cisa.dhs.gov]; [REDACTED]@cisecurity.org]; [REDACTED]@cisecurity.org);  
[REDACTED]@cisecurity.org]; [REDACTED]@cisecurity.org]; [REDACTED]  
[REDACTED]@nased.org]; [REDACTED]@sso.org]; [REDACTED]@sso.org]; [REDACTED]  
[REDACTED]@twitter.com]; [REDACTED]@twitter.com]; [REDACTED]@twitter.com]  
**Subject:** RE: Reporting Portal with CIS, NASS, NASED and Twitter

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

[REDACTED]  
Sorry I am just getting this to you a few minutes before our meeting. We are looking forward to talking through these .

1. Will there be some sort of agreement or terms of reference that will align all participants (reporters, government entities, companies) on objectives and usage of the portal?

Yes, we'll establish Terms of Reference (or equivalent agreements) for the portal. Broadly speaking the objectives are:

- CIS: vet election officials to ensure that all information reported to the platforms comes from the authoritative source for that information.
- Election offices: submit report of misinformation that, as the official authority a certain information, can be stated as factually inaccurate
- Social media companies: process reports and provide timely responses, to include the removal of reported misinformation from the platform where possible
- National associations: maintain awareness of occurrences of misinformation and communicate with other partners as necessary
- Other partners: not on the critical path of the initial rollout; can be discussed as the platform evolves

2. Who will have access to view/analyze reported information? Will there be any restrictions in place to dictate what can be done with this information?

This will be covered in the agreements, which will limit use of data. Broadly speaking usage will be

- CIS: access to all information and ability to analyze and communicate about that information with election offices and social media companies
- Election offices: submit report of misinformation that, as the official authority a certain information, can be stated as factually inaccurate
- National associations: access to all information and ability to analyze and communicate about that information with election offices and social media companies
- Social media companies: Access to reports necessary to investigate and come to a decision
- Other partners: not on the critical path of the initial rollout; can be discussed as the platform evolves

3. Would other companies have access to see reports for other platforms? I believe our answer is no we will not share the reports. However, based on the set of reports, we may share indications of campaigns of misinformation across platforms. What if the report has content from multiple companies? We have it setup where the samples are separated by platform. The top-level report information would be shared with any platform where a sample was provided. We are open to handling this differently and look forward to your thoughts here.

4. What is the criteria used to determine who has access to the portal? The criteria has already been determined (elections officials vetted by CIS, NASS, NASED, DHS and social media platforms). Any others will be on a case-by-case basis with a specific formal terms of access agreement. How many individuals do you anticipate having access? There are roughly 9,000 elections offices. We expect as much as half may participate in the portal over time.

5. How long will reported information be retained?	Redacted Proprietary Information
<b>Redacted Proprietary Information</b>	

6. How long will the portal be in operation? Just through the 2020 presidential election? The portal will be evaluated in January 2021 regarding demonstrated benefits, potential enhancements, and opinions by the elections community regarding continued operation.

7. Companies' terms of service vary. How will individuals know what to report? We will cover this in the Terms of Reference and in the instructions given to users as they use the platform. The elections officials will report suspected misinformation related to elections. The platforms will have to assess the misinformation, including applicability of specific terms of service for the platform.

8. Will there be any quality checks in place? Will there be a review of reports before they are submitted to companies? Will all reports be treated with equal priority? The reporting mechanism has requirements on which fields are required. This validation can be altered based on the "type" of report. We are open to adding more validation based on your feedback. We do not anticipate any manual review of the content itself. The reporter can set a priority, but we should discuss the implications of that to all involved.

9. Will partners continue to use Partner Support Portal (PSP) or will everyone migrate to this reporting tool? We'd like to encourage election officials to use the Reporting Portal, but we believe it makes sense to continue to operate the PSP in parallel through this election and evaluate it afterward.

Thanks,

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[cisecurity.org](http://cisecurity.org)



---

**From:** [REDACTED]@twitter.com>  
**Sent:** Tuesday, June 16, 2020 3:59 PM  
**To:** [REDACTED]@cisecurity.org>  
**Cc:** [REDACTED]@twitter.com>; [REDACTED]@cisa.dhs.gov>; [REDACTED]  
[REDACTED]@cisa.dhs.gov>; [REDACTED]@cisa.dhs.gov>; [REDACTED]  
[REDACTED]@cisa.dhs.gov>; [REDACTED]@cisecurity.org>; [REDACTED]@cisecurity.org>; [REDACTED]  
[REDACTED]@cisecurity.org>; [REDACTED]@nased.org>; [REDACTED]@sso.org>; [REDACTED]@sso.org>; [REDACTED]  
[REDACTED]@twitter.com>; [REDACTED]@twitter.com>; [REDACTED]@twitter.com>  
**Subject:** Re: Reporting Portal with CIS, NASS, NASED and Twitter

All,

Below are some of the questions we hope to discuss during our next call. Looking forward to it!

1. Will there be some sort of agreement or terms of reference that will align all participants (reporters, government entities, companies) on objectives and usage of the portal?
2. Who will have access to view/analyze reported information? Will there be any restrictions in place to dictate what can be done with this information?
3. Would other companies have access to see reports for other platforms? What if the report has content from multiple companies?
4. What is the criteria used to determine who has access to the portal? How many individuals do you anticipate having access?
5. How long will reported information be retained?
6. How long will the portal be in operation? Just through the 2020 presidential election?
7. Companies' terms of service vary. How will individuals know what to report?
8. Will there be any quality checks in place? Will there be a review of reports before they are submitted to companies? Will all reports be treated with equal priority?
9. Will partners continue to use Partner Support Portal (PSP) or will everyone migrate to this reporting tool?

On Fri, Jun 12, 2020 at 3:40 PM [REDACTED] [@cisecurity.org](#) wrote:

[REDACTED]  
Wednesday from 1-2 ET works for our team. I will send an invite.

I will also follow up separately with you on setting up accounts. Have a great weekend.

Thanks,

[REDACTED]  
[REDACTED]  
[REDACTED] [@cisecurity.org](#)



---

From: [REDACTED] [@twitter.com](#)  
Sent: Friday, June 12, 2020 2:29 PM

To: [REDACTED] @cisecurity.org>  
Cc: [REDACTED] @twitter.com>; [REDACTED] @cisa.dhs.gov>;  
[REDACTED] @cisa.dhs.gov>; [REDACTED] @cisa.dhs.gov>;  
[REDACTED] @cisecurity.org>; [REDACTED] @cisecurity.org>;  
[REDACTED] @cisecurity.org>; [REDACTED] @cisecurity.org>;  
[REDACTED] @nased.org>; [REDACTED] @sso.org>; [REDACTED] @sso.org>;  
[REDACTED] @twitter.com>; [REDACTED] @twitter.com>; [REDACTED] @twitter.com>

**Subject:** Re: Reporting Portal with CIS, NASS, NASED and Twitter

Hi [REDACTED]

Thanks again for this group's time yesterday. Can we schedule our next follow-up for next Wednesday from 1-2pm? We'll share some of our questions ahead of that call to help inform our discussion.

Also, would you be able to help us establish some log-ins for us to test out the tool?

Thanks!

[REDACTED]  
On Wed, Jun 3, 2020 at 4:52 PM [REDACTED] @cisecurity.org> wrote:

[REDACTED]  
That works for us here at CIS [REDACTED] will send an invite shortly.

Thanks,

[REDACTED]  
[REDACTED] @cisecurity.org  
[REDACTED]



---

**From:** [REDACTED] @twitter.com>  
**Sent:** Wednesday, June 3, 2020 4:08 PM  
**To:** [REDACTED] @cisecurity.org>  
**Cc:** [REDACTED] @twitter.com>; [REDACTED] @cisa.dhs.gov>;  
[REDACTED] @cisa.dhs.gov>; [REDACTED] @cisa.dhs.gov>;  
[REDACTED] @cisa.dhs.gov>; [REDACTED] @cisecurity.org>; [REDACTED] @cisecurity.org>;  
[REDACTED] @nased.org>; [REDACTED] @sso.org>; [REDACTED] @sso.org>  
**Subject:** Re: Reporting Portal with CIS, NASS, NASED and Twitter

Hi [REDACTED]

Thank you for your patience. Would 3:30 next Thursday (6/11) work for a follow-up call?

Best,

[REDACTED]  
On Mon, Jun 1, 2020 at 8:37 AM [REDACTED] @cisecurity.org> wrote:

[REDACTED]  
I hope you are doing well. I know it is a busy week with the election tomorrow. When you can, please let us know a good time to reschedule our meeting from last week. We will have some updates to share about our beta testing with election officials and a possible nationwide training collaboration with the Belfer Center.

Thanks,

[REDACTED]  
[REDACTED]  
[REDACTED] @cisecurity.org  
[REDACTED]



---

**From:** [REDACTED] @twitter.com>  
**Sent:** Friday, May 22, 2020 4:30 PM  
**To:** [REDACTED] @cisecurity.org>

Cc: [REDACTED]@twitter.com>; [REDACTED]@cisa.dhs.gov>;  
[REDACTED]@cisa.dhs.gov>; [REDACTED]@cisa.dhs.gov>;  
[REDACTED]@cisa.dhs.gov>; [REDACTED]@cisecurity.org>;  
[REDACTED]@cisecurity.org>; [REDACTED]@cisecurity.org>;  
[REDACTED]@cisecurity.org>; [REDACTED]@nased.org>; [REDACTED]@sso.org>;  
[REDACTED]@sso.org>

**Subject:** Re: Reporting Portal with CIS, NASS, NASED and Twitter

Hi [REDACTED]

Thank you for your email and for your time last week. We support your goals in establishing this tool, but still need to run some traps internally regarding options to receive the info and provide feedback. Happy to schedule a follow-up call next week, though we may still have more questions than feedback at that point. If that works for you all, let's aim for 4:30 pm EST.

Best,

[REDACTED]@cisecurity.org> wrote:

Thank you so much for the call last Monday. I hope it proved helpful as you went back to your team at Twitter. With the elections nearing, we are eager to hear if you have anything you can share from your internal conversations. Are you available for a 30 min follow up call next week? We have a few time slots next Thursday if any of these work for you: 9-10am, 2-2:30pm, and 4-5pm (Eastern). If these don't work for you, we can shuffle some schedules around. Just let us know what works best for you.

Thanks,

Dcisecurity.org



-----Original Appointment-----

**From:** [REDACTED] @cisa.dhs.gov>

**Sent:** Wednesday, May 6, 2020 9:31 AM

**To:** [REDACTED]

**Cc:** [REDACTED]

**Subject:** Reporting Portal with CIS, NASS, NASED and Twitter

**When:** Monday, May 11, 2020 2:00 PM-3:00 PM (UTC-05:00) Eastern Time (US & Canada).

**Where:** WebEx invite just sent separately – please use that information

Sent a separate invite to use WebEx for the meeting. Please let me know if you don't receive the WebEx invite.

Thanks,

[REDACTED]

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

.....

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

.....

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

.....

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

.....

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

CONFIDENTIAL

Case 3:22-cv-01213-TAD-KDM Document 71-8 Filed 08/31/22 Page 97 of 111 PageID #:  
2845