From: [redacted]-DNI-
Sent: Friday, September 02, 2016 7:31 AM
To: [redacted]
Cc: [redacted]-DNI-
Subject: FW: NIC product on cyber threats to U.S. electoral infrastructure

Importance: High

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

From: James R. Clapper-DNI-
Sent: Thursday, September 01, 2016 8:16 PM
To: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]-DNI-[redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]>;
[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]
Subject: RE: NIC product on cyber threats to U.S. electoral infrastructure

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted]:

Yes; at the WH session today chaired by Denis, I brought up that I had asked my team to produce an NIE on cyber threats to our electoral infrastructure…this generated quite a bit of discussion. In the end all agreed that some sort of IC product would be VERY useful—exactly what form it would take was left for us to decide. I think where we're headed now is an ICA like product, that could be classified, and then produce an unclass product for wider dissemination at the State/local/tribal levels---which we would provide to DHS/FBI for them to disseminate….

J

From: [redacted]-DNI-
Sent: Thursday, September 01, 2016 9:13 AM
To: James R. Clapper-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]

DNI-[redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]
Subject: NIC product on cyber threats to U.S. electoral infrastructure

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

Jim,

Just wanted to make sure, in all this back and forth, that what we'll do, in the interest of time, is an ICA, NOT an NIE. I assume that is o.k. with you but wanted to make sure. Cheers,
[redacted]

[redacted]

From: [redacted]-DNI-
Sent: Wednesday, August 31, 2016 8:05 PM
To: [redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]
Subject: FW: [redacted] [ACTION] DNI Activity Report -- August 31, 2016

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

Hi [redacted] and cyber team

FYSA -
(U) Election Cybersecurity Support

[redacted] Secretary Johnson committed DHS to supporting state and local agencies to secure computer-enabled election infrastructure. The NCCIC reached out to state and local officials responsible for election infrastructure to offer our assistance in identifying and remediating vulnerabilities. My team is analyzing cyber threats to the upcoming election and, in response to a request from the Special Assistant to the President for Cybersecurity, Michael Daniel, briefed the NSC alongside CIA last week. The brief included a DHS expert on vulnerabilities of the system and overall risk due to cyber incident. We are working with CIA on a PDB submission on the threat. The thrust of the analysis is that there is no

indication of a Russian threat to directly manipulate the actual vote count
through cyber means. However, as seen in recent media reporting, any cyber
activity directed against the election infrastructure is likely to have an
effect on public confidence - even if the cyber operation is unsuccessful or
not intended to impact the election (e.g. theft of PII from a voter
registration database). (J: POTUS agreed yesterday that our electoral
apparatus ((my term)) should be considered as critical infrastructure. I
have directed my folks to generate an NIE on attendant cyber threats to this
key infrastructure, and to get it done sooner than later. Obviously, we
will need to work with your team to produce this.)

I understand that DNI Clapper indicated an NIE on the cyber threats to elections issues, but from our discussion this morning, an ICA should be okay. Our goal is to get an ICA in place by next week given we already worked with CIA and DHS on a variety of cyber threats to election issues. [redacted] is our POC and lead drafter with contributions from DHS, FBI, and CIA.

[redacted]

(U) [redacted]
==
National Intelligence Officer for Cyber Issues
Office of the Director of National Intelligence
[redacted]

-----Original Message-----
From: James R. Clapper-DNI-
Sent: Wednesday, August 31, 2016 7:46 PM
To: [redacted] dhs [redacted]; [redacted] dhs [redacted]
Cc: [redacted] -DNI- [redacted]; [redacted] dhs. [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] cia [redacted]; [redacted] -DNI- [redacted] [redacted]
[redacted] -DNI- [redacted] v>; [redacted] dhs [redacted] >; [redacted] DNI-
[redacted] >; [redacted] -DNI- [redacted] >; [redacted] -DNI- [redacted] >; [redacted]
[redacted] -DNI- [redacted] >; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted] >; [redacted] -DNI- [redacted]
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted] >; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted] [redacted] cia [redacted]; [redacted] dni [redacted];
[redacted] dn [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI- [redacted];
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted] [redacted] -DNI-
[redacted]; [redacted] dhs [redacted]; [redacted] -DNI- [redacted];
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI- [redacted];
[redacted] [redacted] cia [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] dhs [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted]
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI- [redacted];
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] cia [redacted]; [redacted] dni [redacted];
[redacted] dn [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI- [redacted];
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]
Subject: RE: [redacted] [ACTION] DNI Activity Report -- August 31, 2016

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]

===

Thanks, [redacted]...GREAT report.

By the way, I'd like to schedule another visit with you and your team--maybe
do another Townhall...

Some comments embedded....

Jim

-----Original Message-----
From: [redacted]dhs[redacted]
Sent: Wednesday, August 31, 2016 4:09 PM
To: James R. Clapper-DNI-[redacted]
Cc: [redacted]dhs[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]-DNI-[redacted]; [redacted]cia[redacted];
[redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]dhs[redacted];
[redacted]-DNI-[redacted] [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]-DNI-[redacted]; [redacted]-DNI-[redacted];
[redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]cia[redacted]; J[redacted]
[redacted]dni[redacted]; [redacted]dni.[redacted];
[redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]
Subject: [redacted] [ACTION] DNI Activity Report -- August 31, 2016 ---
[redacted]

Classification: [redacted]

Classified By: [redacted]
[redacted] Derived From: [redacted] Declassify On:[redacted]

===

Director Clapper,

I am sending this a bit early as I am off to McAllen TX for a border review.
Here are the issues that I wanted to update : (J: Interested in your
impressions...)

(U) IC ITE Update

[redacted] Last Friday, our IC ITE Team, including representatives from ODNI, reviewed and approved our proposal for a two-phased approach to move forward on IC ITE integration. Phase 1: Replicate in ICITE existing data sharing agreements, using a Community of Interest model. Phase 2: Move to a policy based access model. We are reviewing our requirements with our IC ITE service providers and plan to initially leverage and base our Phase 1 schedule on the ongoing pilot work with WAYWARD SKIES, NCTC, and NCSC - extending to other existing agreements we have with CIA and NSA. Phase 2 requirements are being worked in parallel between DHS and your Policy & Strategy, Mission, and CIO teams. Our next update will take place at the IC CIO Council we are hosting at DHS Headquarters on September 6. (J: I'm repeating myself here, but I again want to thank you for your leadership and persistence here in finding a way-ahead for IC ITE applications. Very appreciative....)

(U) Special Interest Alien (SIA) Joint Action Group (JAG) Follow-Up

[redacted] As previously noted, I led a DHS effort to expand initiatives in order to dismantle human smuggling networks. The secretary received the final brief today and approved the Plan of Action, including increased DHS intel production. We will brief your team on the plan. We are planning to leverage IC ITE to support the SIA JAG. Subject matter experts from NSA, CIA, and the DHS Intel Enterprise are developing a CONOPS that will describe how we can use DHS and IC data (DHS travel and immigration data, along with bulk SIGINT and other IC reporting) with new IC ITE analytics in the cloud. (J: EXCELLENT)

(U/[redacted]) We are examining our current HUMINT collection against this problem set, we may require ODNI assistance in expanding HUMINT collection in key human smuggling transit countries. At present, we do not have immediate additional intelligence requirements from the SIA JAG efforts. (J: Let me know what you need from us....)

(U) Bulk Screening of Social Media Update

(U/[redacted]) The Department's move towards centralized bulk screening capability for social media is a novel, fluid challenge. Since December, we've conducted a number of pilots to test capabilities and developed a process for social media screening. Our intention was to have an initial capability in place by August 1, 2016; however, Congressional feedback required us to rethink our funding strategy. We received Congressional support to continue operational testing on live data, with the intention of achieving initial operating capability in FY2017. Our immediate operational imperatives are Syrian refugees, followed by Electronic System for Travel Authorization (Visa Waiver Program) applicants. We are developing a longer-term funding strategy using fee funds and still intend to house this capability at the CBP/NTC. I will keep you updated as we make progress. (J: Good; please do...)

(U) Election Cybersecurity Support

[redacted] Secretary Johnson committed DHS to supporting state and local agencies to secure computer-enabled election infrastructure. The NCCIC reached out to state and local officials responsible for election infrastructure to offer our assistance in identifying and remediating vulnerabilities. My team is analyzing cyber threats to the upcoming election and, in response to a request from the Special Assistant to the President for Cybersecurity, Michael Daniel, briefed the NSC alongside CIA last week. The brief included a DHS expert on vulnerabilities of the system and overall risk due to cyber incident. We are working with CIA on a PDB submission on the threat. The thrust of the analysis is that there is no indication of a Russian threat to directly manipulate the actual vote count through cyber means. However, as seen in recent media reporting, any cyber activity directed against the election infrastructure is likely to have an effect on public confidence - even if the cyber operation is unsuccessful or not intended to impact the election (e.g. theft of PII from a voter registration database). (J: POTUS agreed yesterday that our electoral apparatus ((my term)) should be considered as critical infrastructure. I have directed my folks to generate an NIE on attendant cyber threats to this key infrastructure, and to get it done sooner than later. Obviously, we will need to work with your team to produce this.)

(U) I&A Internship Program Update

(U) Our 2015-2016 internship program is winding down. Last year, we implemented a structured internship program to meet a number of critical organizational objectives: (1) serve as a pipeline for entry-level employment; (2) assist in diversifying our workforce; and (3) develop well-rounded, I&A intelligence professionals. I am pleased with our progress - since last year, we brought on more than 30 diverse undergraduate and graduate interns from around the country. These interns worked across I&A, both supporting the intelligence cycle and in mission-support functions. In addition to their work, we organized lectures and field trips for them, so they could better understand our various missions. Approximately 20 interns will continue into the school year. We are planning outreach events for next month, in advance of our application period in early October. We are also refining and codifying the program details and intend to broaden our enrichment activities to include the IC next summer. (J: If we can help here, would be pleased to do so. I'd be happy to meet with them...)

(U) Implementation of ICS 704-01 - Issuance of Intelligence Community Badges

(U) We are making progress implementing ICS 704-01. In our initial survey, we found that DHS issued IC badges to more than 4,000 people across the Department, many in non-intelligence roles. Since I issued my guidance in late-May to ensure compliance with the ICS, over 1,465 badges have been turned in and deactivated. I anticipate an additional 1,800 will be deactivated. Once this is complete, less than 1,000 IC badges will remain active throughout the Department - the majority within I&A. Additionally, I&A and the DHS Office of the Chief Security Officer are transitioning the IC Badge System to my Security Management Branch, which will give us greater oversight of badge issuance in the future. (J: Once again YOU ARE MY HERO!! Thanks for this....)

(U) DHS ISR Plan Approved

(U) The DHS ISR Plan was signed last Friday during the Homeland Security Intelligence Council meeting. The ISR Plan lays out the steps to integrate DHS Component ISR data and processes seamlessly, increasing interoperability and providing greater return on investment. The ISR Working Group, comprised of representatives from the DHS Components, will begin implementation of this plan immediately. (J: I gather that what you have done here is to enhance the management of all DHS ISR resources, regardless of which component...do I have that right?)

(U) International Engagement

[redacted] Last Friday, I met with Australian Dept. of Immigration and Border Protection (DIBP) Deputy Secretary for Intelligence and Capability Maria Fernandez. Our discussion focused on establishing analyst-to-analyst assessments on foreign terrorist fighters - a principal action item from the June 2016 U.S.-Australia Strategic Dialogue. We are working on FOUO/LES connectivity via the Homeland Security Information Network and are looking at building SVTC capability with DIBP (similar to the UK Home Office), further enhancing real-time information sharing. We also discussed our countries' respective efforts on creating data lakes for use by operators, ongoing incorporation of social media into the refugee vetting process, and the DIBP's recent development of a predictive modeling mechanism for targeting rules. DS Fernandez and I also agreed to reinvigorate our efforts to meet on a quarterly basis. (J: GREAT out-reach...)

(U) State and Local Engagement

(U) This week, we hosted the inaugural meeting of I&A's State and Local Intelligence Council (SLIC). The SLIC serves as my advisory forum on operational information sharing between I&A and our state and local partners. The SLIC is composed of practitioners from national-level organizations and associations representing a wide range of state and local law enforcement, intelligence, fire service, and emergency management/first responders. We solicited feedback on how I&A can their engagement in our intelligence activities and ensure our production meets their requirements. We also discussed how they can better contribute to our reporting efforts. I will give you a full recap of the discussions, feedback, and recommendations once we complete our after action report. (J: This is great; I am VERY interested in your recap...)

(U) All for now....please let me know if you have questions. (J: Let's set up a working lunch here--to include [redacted]...)

VR,
[redacted]

==
Classification: [redacted]

==
Classification: [redacted]

==
Classification: [redacted]

==
Classification: [redacted]

==
Classification: [redacted]

==
Classification: [redacted]

From: [redacted] (FBI) [redacted]
Sent: Friday, September 02, 2016 11:57 AM
To: [redacted]-DNI-
Subject: RE: [redacted] Cyberthreat to the 2016 Presidential Election - drafting - comments requested by 1100 AM Friday [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted]

Below are inputs from the FBI. Sorry for the delay. Due to the long weekend, we have several folks out.

1) On page 5, under the "(U//[redacted]) Adversaries with Intent" section, we would prefer for the first sentence regarding Russia's intent to be softened. The way it currently reads, it would indicate that we have definitive information that Russia does intend to disrupt our elections and we are uncomfortable making that assessment at this point. We would suggest editing the sentence to read as the following (changes highlighted): "([redacted]) We judge Russia to be the only nation state with the current means and possible motivation to use cyber attack to disrupt the 2016 election or deny political legitimacy to US presidential candidates." We would also suggest editing the title of that section to instead read something along the lines of "(U//[redacted]) Evaluation of Likely Adversaries" so that it doesn't mislead the reader to believe that the IC currently has information indicating Russia has a known intent to influence the elections.

2) We believe it's worth noting that in an extremely close race, it is certainly possible that a very targeted cyber attack aimed at manipulating votes could lead to a change to the legitimate results and affect the outcome of the election. As an example, the votes in a swing county in a swing state could potentially be slightly altered, thus resulting in the electoral college votes of a particular state to go toward one particular individual, thus tipping the entire election in their favor (i.e. in the 2000 election, the results in Florida essentially were decided by one or two counties). Although this is unlikely, it certainly remains a possibility and one that can't be discounted – due to the high impact - even with the disjointed nature of US election technology.

V/R,
[redacted]

[redacted]
Intelligence Analyst
Technology Cyber Intelligence Unit
Cyber Intelligence Section
[redacted]

From: [redacted]-DNI-[redacted]
Sent: Thursday, September 01, 2016 8:50 PM

To: [redacted]; [redacted] (FBI); [redacted] DHS [redacted]; [redacted]; [redacted]-DNI-; [redacted]; [redacted] DHS [redacted]; [redacted] DHS[redacted]; [redacted] DHS [redacted]; [redacted] dhs [redacted]; [redacted] DHS [redacted] [redacted] dhs [redacted]
Cc: [redacted]-DNI-; [redacted]-DNI-Y-; [redacted]-DNI-; [redacted]
Subject: [redacted] Cyberthreat to the 2016 Presidential Election - drafting - comments requested by 1100 AM Friday [redacted]

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
=======================================================
```

[redacted]

Team,

[redacted] Attached please find a draft ICA on *Cyberthreat to the 2016 Presidential Election*. I'm hoping to get inputs from you **tomorrow during the morning**, to enable a fast revision so I can then send it to the broader community around noon. To that end, please note a few things:

1. Note scope language – the NIC does NOT want to write on US vulnerability [and frankly, with this subject, it would take years to get decent data] and though I'd love to write more on the broader influence issue, this product is not the place for that. Please keep that focus in mind when reading the draft so far, and contributing.

2. We are trying to keep this at the strategic level - that said, we are likely missing important reporting or ideas. Please add what you think this needs (but not everything it could contain.) Lower classification data that makes the overall point is preferred to exquisite examples that drive HCS or GAMMA marks – unless it changes the bottom line, in which case have at it.

3. CTIIC – need you folks to help, specifically with some sourcing and an update of your table, and generally regarding other things we may have left out regarding actors or activities.

4. DHS – I would value your thoughts in particular on the language for the page two take on overall proliferation of threats to US cyber, as well as your thoughts on the utility of a tonebox regarding 'warning signs' of hacks-on-election underway.

[redacted] Finally, to all, I feel this draft is especially weak on other actors and intent, for which I take full blame and ask your assistance. Thanks,

[redacted]

[redacted]
NIC, DNIO|Cyber

```
=======================================================
Classification: [redacted]

=======================================================
Classification: [redacted]
```

From: [redacted]-DNI-
Sent: Friday, September 09, 2016 3:40 PM
To: [redacted]-DNI-
Subject: FW: [redacted] RE: Russia and the US Elections

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

(U) [redacted]
==
National Intelligence Officer for Cyber Issues
Office of the Director of National Intelligence
[redacted]

-----Original Message-----
From: [redacted]dhs[redacted]
Sent: Friday, September 09, 2016 12:58 PM
To: [redacted]cia[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]DHS[redacted]; [redacted]FBI[redacted]
[redacted]; [redacted]FBI[redacted]; [redacted]
[redacted]cia[redacted]; [redacted]NSA-[redacted]
[redacted]; [redacted]NSA-[redacted];
[redacted]NSA-[redacted]; [redacted]
FBI[redacted]; [redacted]-DNI-[redacted];
[redacted]DHS[redacted]; [redacted]FBI[redacted]
[redacted]; [redacted]FBI[redacted]; [redacted]
[redacted]cia[redacted]; [redacted]NSA-[redacted]
[redacted]; [redacted]NSA-[redacted];
[redacted]NSA-[redacted]; [redacted]
FBI[redacted]; [redacted]-DNI-[redacted];
[redacted]DHS[redacted]; [redacted]FBI[redacted]
[redacted]; [redacted]FBI[redacted]; [redacted]
[redacted]cia[redacted]; [redacted]NSA-[redacted]
[redacted]; [redacted]NSA-[redacted];
[redacted]NSA-[redacted]; [redacted]
FBI[redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]cia[redacted]; [redacted]
[redacted]cia[redacted]; [redacted]-DNI-[redacted];

[redacted]-DNI-[redacted]; [redacted]
[redacted]cia[redacted]; [redacted]cia[redacted]
Subject: [redacted] RE: Russia and the US Elections ---[redacted]
[redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

I took the intent of this email to get the basic starting point regarding Russia. We agree with: Russia probably is not (and will not) trying to influence the election by using cyber means to manipulate computer-enabled election infrastructure.

Yes, if we're going further, while Russia has some capability to conduct cyber manipulation of election infrastructure, we judge that efforts by them (or others) to change the outcome of an election through cyber means would be detected. That's a key element of our cyber-focused PDB.

We assess that foreign adversaries, notably Russia, are more likely to focus their cyber operations on undermining credibility/public confidence. That assessment feeds directly into the influence operations, some cyber-enabled, that we've seen related to current and historic election cycles. We concur with CIA's change related to that.

[redacted]

Chief, NCCIC Intelligence Support Branch
DHS Office of Intelligence & Analysis (I&A)
[redacted]

-----Original Message-----
From: [redacted]cia[redacted]
Sent: Friday, September 09, 2016 12:26 PM
To: [redacted]-DNI-;[redacted]-DNI-;[redacted];
[redacted];[redacted]FBI[redacted];[redacted]FBI[redacted];[redacted]
[redacted];[redacted]NSA-[redacted];[redacted]NSA-[redacted]
[redacted];[redacted]NSA-[redacted];[redacted]FBI[redacted];[redacted]
[redacted]-DNI-;[redacted];[redacted];[redacted]FBI
[redacted];[redacted]FBI[redacted];[redacted];[redacted]
NSA-[redacted];[redacted]NSA-[redacted];[redacted]
NSA-[redacted];[redacted]FBI[redacted];[redacted]-DNI-;
[redacted];[redacted];[redacted]FBI[redacted];[redacted]
[redacted]FBI[redacted];[redacted];[redacted]NSA-[redacted];

[redacted] NSA-[redacted]; [redacted] NSA-[redacted]; [redacted]
[redacted] FBI [redacted]
Cc: [redacted]-DNI-; [redacted]-DNI-; [redacted]
[redacted]; [redacted]; [redacted]-DNI-; [redacted]
[redacted]-DNI-; [redacted]; [redacted]
Subject: RE: Russia and the US Elections

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==

I defer to [redacted] on the first sentence, but I sort of understood the emphasis to be on Russia probably not having the capability to influence the election. But again, I defer to him. I suggest a tweak to the second sentence.

From: [redacted]-DNI-
Sent: Friday, September 09, 2016 12:05 PM
To: [redacted]-DNI-[redacted]; [redacted] DHS [redacted]
[redacted]; [redacted] DHS [redacted];
[redacted] FBI [redacted]; [redacted] FBI [redacted]
[redacted]; [redacted] cia [redacted]; [redacted]
[redacted] cia [redacted]; [redacted]
[redacted]; [redacted] NSA-[redacted];
[redacted] NSA-[redacted]; [redacted]
FBI [redacted]; [redacted]-DNI-[redacted];
[redacted] DHS [redacted]; [redacted] DHS [redacted]
[redacted]; [redacted] FBI [redacted]
[redacted]; [redacted] FBI [redacted];
[redacted] cia [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] NSA-[redacted]
[redacted]; [redacted] NSA-[redacted];
[redacted] NSA-[redacted]; [redacted]
FBI [redacted]; [redacted]-DNI-[redacted];
[redacted] DHS [redacted]; [redacted] DHS [redacted]
[redacted]; [redacted] FBI [redacted]
[redacted]; [redacted] FBI [redacted];
[redacted] cia [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] NSA-[redacted]
[redacted]; [redacted] NSA-[redacted];
[redacted] NSA-[redacted]; [redacted]
FBI [redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted] cia.[redacted]; [redacted]
[redacted] cia.[redacted]; [redacted]-DNI-[redacted];

[redacted]-DNI-[redacted]; [redacted]
[redacted]cia[redacted]; [redacted]cia[redacted]
Subject: Russia and the US Elections

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

All,

Each of you have PDB or other IC pieces relating to Russia and the US elections. At first read, the pieces seem to say different things. I'm reaching out to see if an agreement can be reached on language. Just as a starting point, would it be accurate to say the below, if not what would be accurate.

Russia probably is not trying to going to be able to? influence the election by using cyber means to manipulate computer-enabled election infrastructure. Russia probably is using cyber means primarily to influence the election by stealing campaign party data and leaking select items, and it is also using public propaganda. This fits an historical pattern of Russia using less sophisticated propaganda and information operations to influence US elections.

[redacted]

[redacted]

Deputy Director / PDB / ODNI

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

===
Classification: [redacted]

===
Classification: [redacted]

===
Classification: [redacted]

===
Classification: [redacted]

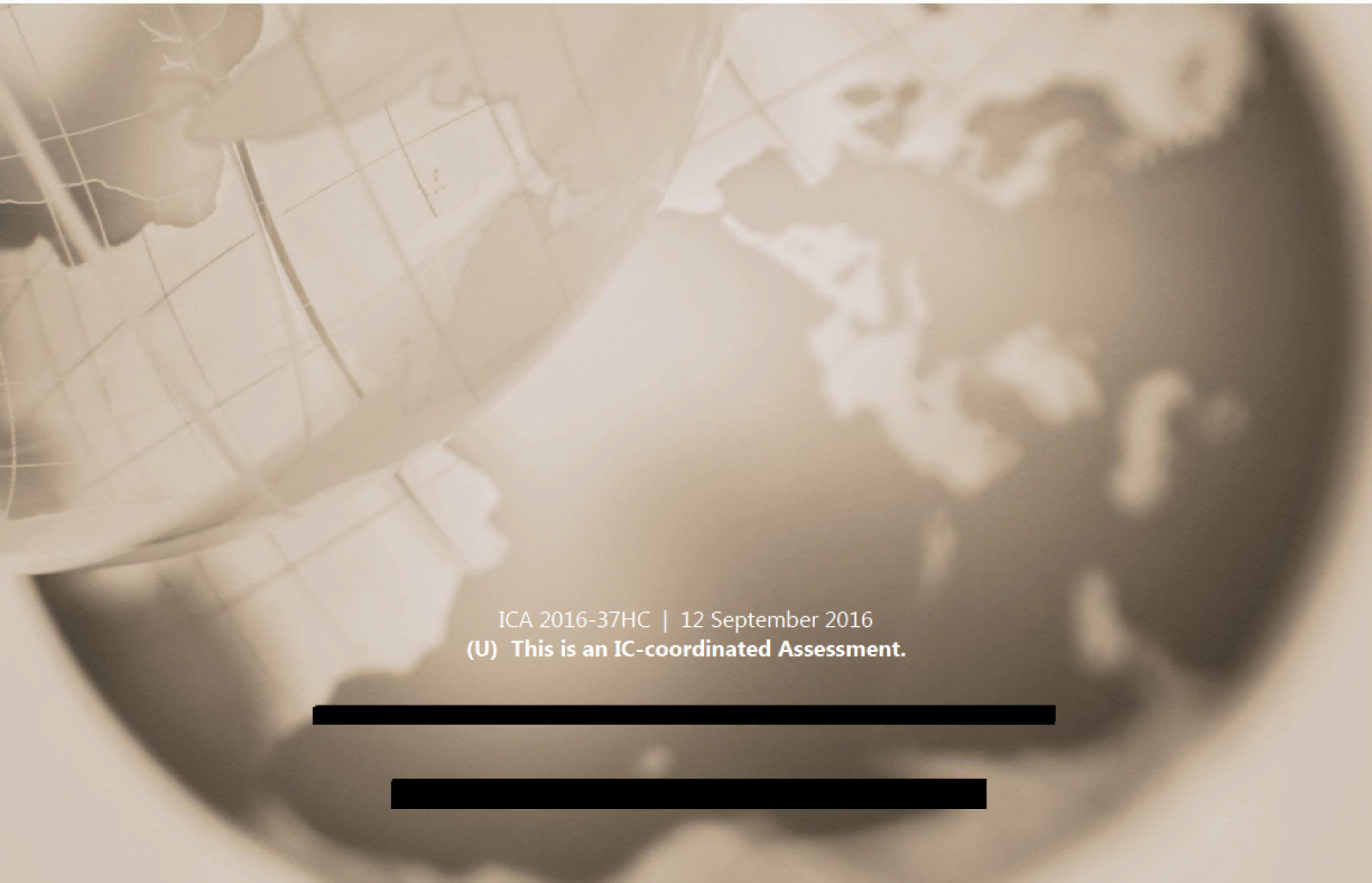
APPROVED FOR RELEASE BY THE DNI ON 17 JULY 2025

[redacted]

ICA

INTELLIGENCE COMMUNITY ASSESSMENT

(U) Cyber Threats to the 2016 US Presidential Election



ICA 2016-37HC | 12 September 2016

(U) This is an IC-coordinated Assessment.

[redacted]

[redacted]

INTELLIGENCE COMMUNITY ASSESSMENT

12 September 2016

(U) This Intelligence Community Assessment was prepared for the National Intelligence Council under the auspices of the National Intelligence Officer (NIO) for Cyber Issues. It was drafted by the NIC, DHS, and CIA with contribution from the CTIIC and coordinated with DHS, FBI, CIA, DIA, NGA, NSA, and State/INR. Questions about this assessment may be directed to the NIO on secure [redacted] *or unsecure* [redacted].

[redacted]

[redacted]

[redacted]

(U) Cyber Threats to the 2016 US Presidential Election

(U) Key Insights

[redacted] **We judge that foreign adversaries do not have and will probably not obtain the capabilities to successfully execute widespread and undetected cyber attacks on the diverse set of information technologies and infrastructures used to support the November 2016 US presidential election.** We have only moderate confidence in our overall threat assessment, [redacted]

[redacted] **The most likely cyber threat to the election is from low-level, detectable, cyber intrusions and attacks that cause localized disruption but do not threaten the overall functionality of the election services or infrastructures.** Nonetheless, even the perception that such low-level intrusions and attacks have occurred risks undermining public confidence in the legitimacy of the electoral process, the validity of the election's outcome, and the mandate of the winning candidate. **We further assess that foreign adversaries are more likely to focus election-related cyber operations on undermining the credibility of the electoral process than on clandestinely manipulating the vote outcome through cyber means.**

[redacted] **We judge that Russia, China, Iran, and North Korea can execute a variety of disruptive cyber attacks, including data corruption, distributed denial of service, and even data modification on some election infrastructure.** Depending on the adversaries' level of access and the targeted system's vulnerabilities, some nation states and non-state actors could probably corrupt or deny many online election services, modify or delete entries in Internet-connected voter registration databases, and corrupt some electronically cast or tabulated votes in some voting precincts. Adversaries might also target the most contested or decisive locales and voting blocs in order to maximize the psychological impact of cyber attacks**. Although unlikely, in a "perfect storm," a cyber adversary might be able to target a small number of critical counties in highly contested states with significant numbers of Electoral College votes, potentially altering the apparent outcome of and almost certainly undermining public confidence in the election.**

[redacted] **We judge Russia has conducted cyber and intelligence operations that suggest that it has potential interest in disrupting the US presidential election**. The Kremlin's cyber penetration of a US political party's servers and the timing of the probable subsequent leak of stolen data suggest that Russia is motivated to exploit the period surrounding the US presidential election either to try to shape the US political environment or to advance other Russian interests. For example, Putin might simply wish to make the US electoral process appear illegitimate or to undermine the legitimacy of the President-elect, in order to strengthen Moscow's hand.

[redacted] **We judge that although it has the means to do so, China is unlikely to publicly release any materials that it might have collected from campaigns or candidates and that it will probably not attempt to influence the outcome of this presidential election via cyber means.** We make this judgment with low confidence [redacted]

(U) Contents

(U) Discussion

(U) Annexes

(U) Scope Note

(U) Information available as of 8 September 2016 was used in the preparation of this product. This ICA addresses the period between 8 September 2016 and 9 November 2016. Judgments might be revised during this timeframe if our understanding of adversaries' capabilities and intentions significantly change.

[redacted] This ICA assesses the threat from and likely objectives of cyber attacks conducted by foreign state and non-state actors against the 2016 US presidential election.

[redacted] This paper does not provide a comprehensive overview of all cyber-enabled efforts to influence US or foreign voter perceptions. By influence, we mean an attempt to shift perceptions of a target group, sow doubt or a loss of trust in targeted social or political institutions, or effect a change in behavior or action of a target group. Additional IC products addressing this issue include:

- [redacted] [redacted].
- [redacted] [redacted]
- (U) ODNI, Spring 2015; *(U) Cyber War, Netwar, and the Future of Cyberdefense*; document is UNCLASSIFIED.

(U/[redacted]) [redacted]

(U) Assumptions

- (U) The cybersecurity of IT systems used in the 2016 presidential election will be at best comparable to the security of federal government IT systems.
- (U) No responsible entity will make any significant change that affects the connectivity of the domestic Internet infrastructure and the global Internet.
- (U) US policy regarding responses to cyber attack will not significantly change.

(U) Estimative Language

(U) Estimates of Likelihood convey judgments about the probability of developments or events. Confidence Levels provide assessments on the quality and quantity of source information. Annex D (Estimative Language) elaborates on these terms. We have "moderate confidence" in all judgments except as otherwise noted.

(U) Cyber Threats to the 2016 US Presidential Election

(U) Discussion

[redacted] We have no indication that foreign adversaries are planning to manipulate or sabotage computer-enabled US election infrastructure. **We assess that foreign adversaries—most notably Russia—probably expect cyber operations against US election infrastructure to be more effective in undermining the legitimacy of the process and the winning candidate than in covertly manipulating the vote outcome.**

- [redacted] Although many adversaries are capable of detectable, disruptive cyber attacks against computer-enabled US election infrastructure, **it is most likely beyond the means of our adversaries to use cyber attacks to affect a covert and widespread shift of the recorded votes to decisively favor a particular candidate during the 2016 US presidential election.** This is not because adversaries lack considerable capabilities but because the US electoral process is a highly decentralized, procedurally and technologically diverse activity and because the will of the voting public is itself dynamic, shifting up to the day of the election. These factors would make it difficult, although not impossible, for even highly capable adversaries to identify and target enough ultimately decisive critical nodes in advance.

[redacted] Clandestine, Widespread Manipulation of Election Results Likely Beyond Capability of Adversaries

[redacted] **Key Judgment 1. We judge that foreign adversaries do not have and will probably not obtain the capabilities to successfully execute widespread and undetected cyber attacks on the diverse set of information technologies and infrastructures used to support the November 2016 US presidential election.** We have moderate confidence in our overall threat assessment, [redacted]

- [redacted] Experts at a June 2016 conference sponsored by the US Government to analyze cyber threats to e-democracy suggested that **the decentralized nature of the US election system is a potential source of strength**. Although lamenting that the United States lacks centralized standards for its voter registration and voting systems, the experts asserted that the diversity of existing technical solutions, as well as the decentralized nature of the systems and the election process, create resilience. No single technical solution has been adopted across the entire country; instead, approaches differ widely across different localities, even within states, resulting in decentralized voting procedures and a variety of machines. As a result, **the potential impact of system-specific cyber exploits would probably be limited, and an adversary would need to compromise multiple systems in multiple locations to alter outcomes in a national election**.

- (U//[redacted]) These experts further concluded that **data from legitimate elections generally exhibits statistical characteristics that can be measured against other elections, enabling detection of fraud in the weeks following an election**. Anomalous voting behavior is not always an indicator of fraud, and hiding some signatures of fraud is possible if the fraudster is aware of the signatures in question. However, experts believed that it would be difficult to conceal the full range of anomalies that a large-scale manipulation of votes would generate.

- (U//[redacted]) Cyber operations against electronic voting machines, particularly those that do not provide a paper record of individual votes for auditing purposes, would be the most effective way to manipulate the votes without being detected, according to research by other academic and industry experts. These systems are usually not connected directly to the Internet, however, and to affect them would require physical access, supply chain compromise, or insider-enabled operations. The resource-intensive nature of such operations would make them difficult to conduct on a large scale.

- **(U//[redacted]) System diversity and existing safeguards would be likely to prevent the undetected manipulation of election results, according to DHS. However, multiple technical pathways exist to undermine public confidence in the electoral process.** These include manipulation of voter eligibility lists, exploitation of electronic voting machines that lack voter-verified paper audit trails, and compromise of election night reporting systems.

(U//[redacted]) Low-Level, Detectable Attacks Pose Most Likely Threat

[redacted] **Key Judgment 2. The most likely cyber threat to the election is from low-level, detectable, cyber intrusions and attacks that cause localized disruption but do not threaten the overall functionality of the election services or infrastructures.** Nonetheless, even the perception that such low-level intrusions and attacks have occurred risks undermining public confidence in the legitimacy of the electoral process, the validity of the election's outcome, and the mandate of the winning candidate. **We further assess that foreign adversaries are more likely to focus election-related cyber operations on undermining the credibility of the electoral process than on clandestinely manipulating the vote outcome through cyber means.**

- [redacted] Adversaries interested in decreasing voter confidence might be encouraged by the open questioning of the cybersecurity of the upcoming US election, based on numerous news and editorial reports in major media outlets globally since summer 2016. Historically, Russian, Iranian, and North Korean operators who engage in cyber-enabled influence operations have focused on maximizing media reporting on an incident in order to discredit or undermine victims. Growing public concern over the vulnerabilities of the US election systems would probably feed potentially sensationalized coverage of even local, low-level cyber attacks. This could enhance the impact of even low-level intrusions that are detected and publicized.

- [redacted] Cyber activists might attempt disruptive cyber attacks, such as distributed denial of service (DDoS) attacks or web defacements, in the lead-up to and potentially during vote processing.

- [redacted] We judge that—even without linkage to any plan or intent to disrupt an election—criminals will continue to use cyber means to steal voter registration data, given previous operations targeting bulk personally identifiable information (PII). **The compromise of voter registration data even for**

petty criminal purposes could be leveraged by other actors seeking to disenfranchise a body of voters via cyber means. In addition, in its early stages, criminal compromise might be indistinguishable from an effort to disrupt and might be portrayed as evidence of registrant manipulation even when no manipulation actually occurred.

- [redacted] **A variety of perpetrators—from nation-state adversaries to novice, domestic cyber criminals—might use some of the same cyber tactics, techniques, and procedures. Because of this, indications of a cyber attack during the election, in isolation, would not necessarily be the result of foreign interference.**

[redacted] Targeted Attack Within the Reach of Many Adversaries

[redacted] **Key Judgment 3. We judge that Russia, China, Iran, and North Korea can execute a variety of disruptive cyber attacks, including data corruption, distributed denial of service, and even data modification on some election infrastructure.** We further assess that almost all current and potential cyber adversaries—nations, criminal groups, terrorists, and individual hackers—now have a range of capabilities to exploit and, in some cases, attack unclassified access-controlled US and Allied information systems via remote penetration from the Internet. We have high confidence in our judgments based on a body of reporting that reveals adversaries' abilities to penetrate and manipulate a wide variety of US systems.

- [redacted] US IC and law enforcement organizations are currently analyzing successful cyber intrusions into two state election networks and attempts into at least three others that have occurred since mid-2015 (see Annex A). We do not know the identity of the perpetrators, and at this time we are aware of only the theft of data—not data deletion or modification—as a result of these incidents. These intrusions, foreign interest in election-associated PII, and the demonstrable vulnerability of the related systems all suggest there is a significant risk of additional incidents.

- [redacted] Historically, Russia, China, Iran, and North Korea have been able to compromise a wide variety of the Internet-connected federal government networks, despite US cybersecurity efforts.

- [redacted] Because we assume that the cybersecurity of IT systems to be used for the 2016 election is comparable to the cybersecurity of federal networks, we judge that with sufficient preparation and system access, our adversaries probably could corrupt or deny many online election services and systems. Services that could be attacked during the election include information on poll locations, status, and closing times, as well as the post-election calculation of results. Adversaries could also preemptively modify or delete entries in networked voter registration databases and—if vulnerable IT systems were employed—corrupt some electronically cast or tabulated votes in some voting precincts.

- [redacted] Alaska—which allows submission of online absentee ballots from any Alaskan voter—might be a particularly attractive target. Adversaries might attempt a DDoS attack to prevent the upload of ballots, seek to corrupt data in the Internet's domain name servers (DNS) or routing tables to redirect would-be voters to non-existent or fraudulent websites, or to manipulate the vote through man-in-the-middle attacks or by compromising the voting servers. Although such efforts would probably ultimately be detected, they might disenfranchise significant numbers of voters. In addition, even unsuccessful attacks would erode confidence in the election process, providing opportunities to adversaries to cast doubt upon the legitimacy of both the process and results.

[redacted] Despite the diverse nature of the computer-enabled US election infrastructure and the difficulties associated with anticipating decisive tipping points in advance—in cases where an election is decided by a few closely contested areas that also employ vulnerable technologies—a targeted cyber attack on these locations might have significant impact on public confidence in the election or even actually be able to shift the overall outcome. **If a "perfect storm" of coincident political and technological sensitivity were to develop, a cyber adversary might be able to target a small number of critical counties in highly contested states with significant numbers of Electoral College votes. This could potentially alter the apparent outcome of, and almost certainly undermine public confidence in, the election.** Although we understand this scenario is unlikely, it remains a possibility that we cannot discount.

[redacted] We judge that most adversaries could develop sufficient understanding of the US political system to enable identification and targeting of the most contested or decisive locales and voting blocs. **They might use this insight to focus and maximize the psychological impact of even minor cyber attacks on the election.**

- [redacted] Such attacks might be used to selectively disenfranchise—for example, by preemptively corrupting records of a particular group of voters or by manipulating public websites to give false information about the closure, relocation, or acts of violence at specific polling locations. Such misinformation might deter participation or flood some polling locations with more voters than they could support.

- [redacted] Targeted cyber attacks might also be used to compromise the actual vote, or its tabulation, in key precincts that employ vulnerable systems. Both state and non-state actors probably have the ability to determine, research, and defeat—via remote or insider means—selected systems in some locations.

- [redacted] Adversaries could exploit open source information, information acquired via cyber theft, and commercially available bulk data sets to support targeting efforts against cyber-enabled election infrastructure.

- [redacted] Adversaries could take advantage of a wide variety of open source information on emerging swing districts, county voting equipment, and other targeting details provided by news companies, voting rights organizations, and other nongovernment organizations (NGOs). For example, a US news website reported in September 2016 that voters ". . . in four competitive states will cast ballots . . . on electronic machines that leave no paper trail . . ." and further noted that ". . . potential trouble spots include Pennsylvania, where the vast majority of counties still use ATM-style touchscreen voting machines without the paper backups that critics . . . began demanding more than a decade ago."

- [redacted] Adversaries could also use cyber espionage operations to obtain non-public information acquired from candidate campaign organizations, political parties, and state and local governments on issues like voting trends, election equipment, and vulnerable districts and systems. The IC does not know the details of the information stolen during recent Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC) hacks, but notes that open sources suggest sensitive, election-related, non-public information was obtained.

- [redacted] Bulk data sets that might be used to identify key precincts or voting groups might be available from commercial data aggregation sources, either directly or via cyber espionage. In October 2015, a Russian speaking cybercriminal was selling a database of PII from more than 190 million US persons from 49 states, claiming that the data had been copied from a "central server of the election commission." [redacted]

[redacted] Russia: Potential Interest in Disrupting US Election

[redacted] **Key Judgment 4. We judge Russia has conducted cyber and intelligence operations that suggest that it has potential interest in disrupting the US presidential election.** Russia is probably the most capable and willing actor to conduct such operations based on its probable involvement in US election-related disclosures, the downward trend the bilateral relationship, and Russian leaders' deeply held belief that Washington has tried to influence past Russian elections.

- [redacted] We assess that Russian intelligence services were behind the compromises of the DNC and DCCC networks and of email accounts from members of Congress, state political parties, a voter registration organization, and seven other US political organizations. We have high confidence in our assessment [redacted]

[redacted] Cyber operations are only one component of a multifaceted toolkit the Russians employ to influence the outcome of elections in other countries. Russia also uses general media messaging to promote or disparage candidates and other tools, some of which we judge would be more difficult for the Kremlin to replicate in the United States. (See Annex C: Moscow's Efforts To Manipulate Foreign Elections, 2000-2016.) Cyber influence operations that involve the release of compromising or embarrassing information—whether true or fabricated—are force multipliers for Moscow's media messaging. They can be used to grab headlines quickly in what is otherwise a very open and diverse US media environment in which the Kremlin cannot control the message as easily as in other countries.

- [redacted] We assess that the Russian services probably orchestrated at least some of the disclosures of DNC and DCCC documents from June to August 2016. Our assessment is based on the timing of the disclosures and the fact that Russian intelligence was in possession of the leaked information from both the DNC and DCCC that the online persona "Guccifer 2.0" claimed to have provided.

- [redacted] FBI and NSA, however, have low confidence in the attribution of the data leaks to Russia. They agree that the disclosures appear consistent with what we might expect from Russian influence activities but note that we lack sufficient technical details to correlate the information posted online to Russian state-sponsored actors.

[redacted] **If the disclosures of the DNC and DCCC documents were indeed orchestrated by the Russian intelligence services, those services would very likely have sought Putin's approval for the operation.** We make this assessment because of the expected, high-profile nature of the resulting controversy, and the high likelihood that the disclosure would be linked to Russia because of open source reports about Russian involvement in the DNC and DCCC hacks.

- [redacted] Proposals for more routine Russian information operations might originate with the central apparatuses of intelligence services or their officers in the field, senior officials within Russian Government entities such as the Presidential Administration, or from Kremlin-linked think tanks. [redacted]

[redacted] **The Kremlin's cyber penetration of a US political party's servers and the timing of the probable subsequent leak of stolen data suggest that Russia is motivated to exploit the period surrounding the US presidential election either to try to shape the US political environment or to advance other Russian interests.** For example, Putin may simply wish to make the US electoral process appear illegitimate, or to undermine the legitimacy of the President-elect, in order to strengthen Moscow's hand. President Putin has the will and the authority in the Russian system to act forcefully and opportunistically —and sometimes without planning for all the consequences—as he showed in occupying and annexing Crimea.

- [redacted] The Kremlin probably expects that publicity surrounding the leaked party data will raise questions about the integrity of the US political process, as Putin hinted in a recent interview.

[redacted] China: No Indication of Plans To Use Cyber Operations To Influence US Election

[redacted] **Key Judgment 5. We judge that although it has the means to do so, China is unlikely to publicly release materials that it might have collected from campaigns or candidates and that it will probably not attempt to influence the outcome of the presidential election via cyber means.** We make this judgment with only low confidence, [redacted]

- [redacted] Chinese [redacted] cyber operators targeted the networks of candidates for the 2008 and 2012 presidential elections and exfiltrated candidates' e-mails, [redacted] After the intrusions, China did not publically release information. [redacted]

- [redacted] Recent reporting underscores China's ongoing interest in gaining insights into the policies of US presidential candidates; [redacted]

- [redacted] [redacted] the eight gigabytes (GB) of emails of a named presidential candidate, staff, and party officials, [redacted] We assess that these emails refer to the records made public by WikiLeaks on 22 July, based on the timing of the inquiry and the size of material. [redacted]

[redacted] Other State Actors' Threat to US Election: Possible but Unlikely

[redacted] [redacted]

- [redacted] **Iran** might be motivated to try to undermine US electoral legitimacy in retaliation for perceived US hostility; Iran claims that the United States is failing to uphold the spirit of the Joint Comprehensive Plan of Action (JCPOA) and is increasingly aggressive against Iranian interests. Iran has previously leaked information that it thinks will damage or embarrass its adversaries and has used fake groups to claim credit for cyber operations. [redacted]

- [redacted] **North Korea** has a general intent to discredit and embarrass the United States. As a result, Pyongyang might view the election and transition period as a window of opportunity for its own agenda. [redacted] However, North Korea's attack on Sony Entertainment in 2015 and its public release of personal and confidential information provides a template for similar operations should Pyongyang seek to influence the US election.

[redacted] **Foreign adversaries** seeking to use stolen information as a means to influence or disrupt the US election could use multiple online platforms—such as WikiLeaks—that have a record of protecting sources to avoid attribution. However, a state adversary would be likely to consider the risk of appearing to influence US elections and the impact on its own public image if it were caught or implicated. [redacted]

[redacted] Non-State Actors With Capabilities To Influence US Election

[redacted] Multiple non-state actors, including cyber activists and the "Islamic State of Iraq and the Levant" (ISIL), might desire to disrupt the 2016 US election to undermine the political legitimacy of the candidates based on these groups' past behavior. We have limited reporting suggesting some historic ISIL access to foreign voter databases, but we currently lack specific reporting to suggest that any non-state actor is either planning or preparing to disrupt the 2016 presidential election via cyber attack.

- [redacted] [redacted]

[redacted]

[redacted] Some companies conduct hacking-for-hire operations in support of political and commercial covert influence campaigns, which could empower unknown opponents.

- [redacted] The Indian security company Appin has acted on the behalf of clients to delete or disrupt communications to influence public perceptions of political parties in Africa, Asia, the Caribbean, and Latin America, [redacted]

- [redacted] [redacted]

[redacted] However, we lack reporting about either the planning or preparation for commercial hacking firms to be used against the US presidential election in 2016.

[redacted] Annex A—Possible State-Level Election Network Breaches and Related Intrusions

(U) This table is classified [redacted]

State	Date of Reported Discovery	Details	Compromise Confirmed?	Data Exfiltrated? (Type)
Arizona	June 2016	(U//[redacted]) A state employee's credentials used by an unknown actor to view voter registration data over a three-day period, according to press reporting. No evidence voter registration data was modified, according to DHS; credentials were posted on an online forum.	Yes	No
Florida	August 2016	(U) Multi-State Information Sharing and Analysis Center (MS-ISAC) reported the Florida State Board of Elections website communicated with one of the same Internet Protocol (IP) addresses that targeted the Maryland State Board of Elections in August 2016 (see below), according to DHS.	No	No
Illinois	July 2016	(U//[redacted]) Compromise of the state voter registration system via SQL injection and credential theft, [redacted]. Up to 200,000 voter records retrieved, according to press reporting. No data altered, according to press reporting and DHS.	Yes	Yes (Voters' names, addresses, last four social security digits, birthdates, and either driver's license numbers or state ID numbers)
Maryland	August 2016	(U/[redacted]) Maryland State Board of Elections officials discovered IP addresses targeting their network via SQL injections after reviewing an MS-ISAC report regarding election compromises, according to DHS. There is no evidence of a compromise; however, as a precaution, the DHS National Cybersecurity and Communications Integration Center (NCCIC) retrieved images from two servers for analysis and investigation. The breach involved the same IP addresses that targeted the Illinois voter registration system.	No	No
North Dakota	August 2016	(U/[redacted]) MS-ISAC notified NCCIC that state officials had identified malicious activity on voting infrastructure from IPs and URLs documented in an MS-ISAC Cyber Alert, according to DHS. MS-ISAC reported that the same IPs and URLs were found in the Maryland and Illinois incidents.	Yes	Unknown
Ohio	August 2016	(U/[redacted]) The MS-ISAC informed NCCIC of a potential compromise of the Ohio voter registration database. FBI spoke with the Ohio Board of Elections (BoE) and determined that voter registration information was available through a public FTP site. The Ohio BoE has since disabled the FTP site.	No	Possibly (Voter database)
Pennsylvania	March 2016	(U) An individual was attempting to sell on an Internet forum a database purportedly containing 600,000 Pennsylvania voter information records, according to a report from an information security firm.	No	Possibly (Voter database)
"State voter registration organization"	June-July 2016	([redacted] Signals intelligence indicates that actors associated with the Russian military intelligence (GRU) in June collected e-mail content from a voter registration organization.	Yes	Yes (E-mail content)
Other—Election commission central server	October 2015	(U/[redacted]) A Russian-speaking cybercriminal offered to sell a database containing the personal information of approximately 190 million US persons from 49 states, [redacted]. The cybercriminal claimed the database had been copied from a "central server of the election commission"—the list of people who had voted in the election. However, an ongoing US Secret Service investigation revealed that the data is an aggregation of publicly available voter registration data which the criminal appeared to have obtained from a US company.	No	No
Democratic National Committee (DNC)	July 2015	[redacted] Russia's Foreign Intelligence Service (SVR) established a presences in the DNC network in July 2015 and exfiltrated data in March 2016, [redacted] GRU accessed the network in May 2016, [redacted]	Yes	Yes (Various)
Democratic Congressional Campaign Committee (DCCC)	April 2016	[redacted] GRU malware was identified on the DCCC network, according to FBI reporting.	Yes	Likely

[redacted]

(U) Annex B
[redacted] Vulnerability of Computer-Enabled Election Systems to Manipulation

Page 1 of 2

[redacted] Computer-enabled election systems are vulnerable to manipulation or disruption at various points, but redundancies in the system and problems with scale would probably make it difficult for cyber actors to affect the outcome of an election without being detected, especially a US presidential election. Rather than trying to covertly change the actual outcome of an election, potential adversaries are more likely to use cyber operations against election systems to undermine the credibility of the process and weaken the perceived legitimacy of the winning candidate.

(U) This table is [redacted]

	VULNERABILITY TO MANIPULATION	DOMESTIC EXAMPLE OF RISK
Voter records	Cyber actors could delete, manipulate, or deny access to voter records to selectively suppress voting; however, backup records can mitigate effects of such activity if manipulation is detected before voting starts.	States employ three methods of maintaining voter registration databases: managed by the state, managed by localities, or hybrid. State-managed systems have greater potential for larger scale manipulation, due to the centralization of records; however, state-level cyber security is often better than that of localities. A recent compromise of state voter registration systems indicates theft of data, rather than manipulation of records.
Online ballot returns	These are often restricted to overseas citizens and are therefore limited in terms of scalability, but their online nature puts them at more risk than other computer-enabled parts of the election system.	Alaska allows all voters to submit an absentee ballot electronically; 24 additional states (e.g., Colorado, Iowa, Missouri, North Carolina) and the District of Columbia allow voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) to submit ballots via e-mail or Internet portal. The Department of Defense projects 154,000 UOCAVA votes—0.1 percent of ballots cast in 2012—will be submitted electronically in 2016.

[redacted]

[redacted]

(U) Annex B
[redacted] Vulnerability of Computer-Enabled Election Systems to Manipulation

Page 2 of 2

(U) This table is [redacted]

	VULNERABILITY TO MANIPULATION	DOMESTIC EXAMPLE OF RISK
Electronic voting systems	Electronic voting systems that do not provide a paper audit trail would provide the best opportunity for covertly manipulating the outcome of an election. However, they are usually not directly connected to the Internet and would require resource-intensive supply chain, insider-enabled, or close access operations to misregister votes or disrupt voting on a large scale.	Counties and parishes within 16 states (e.g., Florida, Indiana, Louisiana, New Jersey, Pennsylvania, Texas, Virginia) employ electronic voting systems without a paper audit trail, although many of these jurisdictions employ other forms of voting as well. There are about 61.5 million registered voters who vote in these jurisdictions.
Local or state compilation	Computer-enabled systems to tabulate votes recorded on paper-based ballots are often used to count votes at the local level.	Almost every county in the United States employs computer-enabled tabulation of some kind. With some exceptions (e.g., where ballots are destroyed following initial optical scans, or in the case of paperless electronic voting machines), officials can recount by hand if verification checks suggest discrepancies in the tabulation process.
Transmission to county or state election authorities	Denial-of-service attacks or other disruptive operations could temporarily disrupt online transmission of vote results, but officials could use alternate means to share them, such as telephonically. Additionally, network-enabled systems that aggregate votes at the local, county, or state level are potentially vulnerable to manipulation, but discrepancies between tallies increase the likelihood that any large-scale manipulation would be exposed.	Most states rely on public telecommunications infrastructure to transmit vote results, although some have dedicated infrastructure that can be used. Centralized locations tabulating multiple precincts' votes provide opportunities for larger scale vote manipulation. Some states are using cloud services—online infrastructure purchased from private-sector providers—to transmit results, as well as to count and log votes.
Public dissemination of voting results . . .	. . . featuring national vote tallies are relatively accessible; election authorities would notice the discrepancy and correct it quickly.	Each state employs its own vote reporting system, generally called an Election Night Reporting System. These systems can be vendor-provided solutions or developed by a state. Many states use cloud services to host results on election night because of the significant demand during that period.

[redacted] [redacted]

(U) Annex C

[redacted] Moscow's Efforts To Manipulate Foreign Elections, 2000-16

[redacted] Moscow uses a diverse toolkit of overt and covert measures to try to influence elections abroad by denigrating opponents and manipulating the election process. Moscow since at least 2000 has tried to influence elections in what it views as its sphere of influence, more recently broadening its efforts to include Europe. This chart and map below highlight examples of election manipulation with evidence of a direct link to Moscow.

(U) RUSSIA'S TOOLBOX

[redacted] We have identified six primary tools that Moscow uses to manipulate foreign elections; Russian officials base tool use on a variety of factors, including geographic distance and Russia's levers of influence in the region.

[redacted]

LOCATION OF INFLUENCE

🟥 Eurasia 🟦 West-Central Europe

MEASURE

Advisers
Providing advisers to assist in campaigning

Cyber
Deploying technical cyber capabilities to influence an election

Economic levers
Using import/export restrictions, worker visas, or energy resources to influence an election

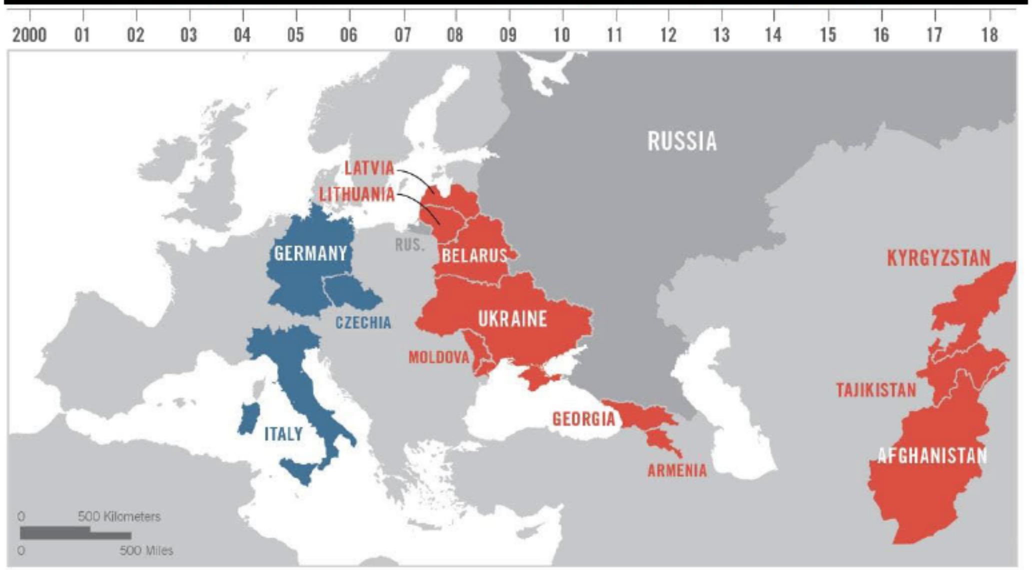
Funding
Providing money to campaigns or candidates

Messaging
Using media to promote a candidate, spreading disinformation, or releasing compromising information

Public backing
Sponsoring candidates' travel to Moscow or expressing public support for candidates

[redacted]

[redacted]



[redacted] [redacted]

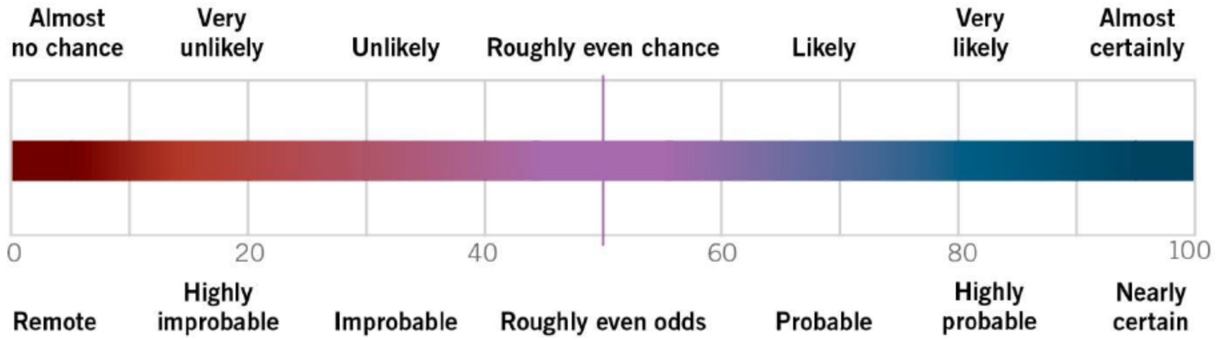
(U) Annex D

(U) ESTIMATIVE LANGUAGE

(U) Estimative language consists of two elements: judgments about the likelihood of developments or events occurring and levels of confidence in the sources and analytic reasoning supporting the judgments. Judgments are not intended to imply that we have proof that shows something to be a fact. Assessments are based on collected information, which is often incomplete or fragmentary, as well as logic, argumentation, and precedents.

(U) **Judgments of Likelihood.** The chart below approximates how judgments of likelihood correlate with percentages. Unless otherwise stated, the Intelligence Community's judgments are not derived via statistical analysis. Phrases such as "we judge" and "we assess"—and terms such as "probable" and "likely"—convey analytical assessments.

Percent



(U) **Confidence in the Sources Supporting Judgments.** Confidence levels provide assessments of the quality and quantity of the source information that supports judgments. Consequently, we ascribe high, moderate, or low levels of confidence to assessments:

- (U) **High confidence** generally indicates that judgments are based on high-quality information from multiple sources. High confidence in a judgment does not imply that the assessment is a fact or a certainty; such judgments might be wrong.
- (U) **Moderate confidence** generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
- (U) **Low confidence** generally means that the information's credibility and/or plausibility is uncertain, that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that reliability of the sources is questionable.

(U) National Intelligence Council

The National Intelligence Council manages the Intelligence Community's estimative process, incorporating the best available expertise inside and outside the government. It reports to the Director of National Intelligence in his capacity as head of the US Intelligence Community and speaks authoritatively on substantive issues for the Community as a whole.

NIC Leadership

Chairman	[redacted]	[redacted]
Vice Chairman	[redacted]	[redacted]
Counselor/Director, Analysis and Production Staff	[redacted]	[redacted]
Chief of Staff	[redacted]	[redacted]
Director, Strategic Futures Group	[redacted]	[redacted]

National Intelligence Officers

Africa	[redacted]	[redacted]
Counterintelligence	[redacted]	[redacted]
Cyber Issues	[redacted]	[redacted]
East Asia	[redacted]	[redacted]
Economic Issues	[redacted]	[redacted]
Europe	[redacted]	[redacted]
Iran	[redacted]	[redacted]
Military Issues	[redacted]	[redacted]
The Near East	[redacted]	[redacted]
North Korea	[redacted]	[redacted]
Russia and Eurasia	[redacted]	[redacted]
South Asia	[redacted]	[redacted]
Space & Technical Intelligence	[redacted]	[redacted]
Technology	[redacted]	[redacted]
Transnational Threats	[redacted]	[redacted]
Weapons of Mass Destruction and Proliferation	[redacted]	[redacted]
Western Hemisphere	[redacted]	[redacted]

UNCLASSIFIED

(U) National Security Information

(U) Information available as of 8 September 2016 was used in the preparation of this product.

(U) The following intelligence organizations participated in the drafting of this product:

National Intelligence Council
Department of Homeland Security, Office of Intelligence and Analysis
Central Intelligence Agency

(U) The following intelligence organizations participated in the coordination of this product:

Central Intelligence Agency
Defense Intelligence Agency
National Geospatial-Intelligence Agency
National Security Agency
Department of Homeland Security, Office of Intelligence and Analysis
Department of State, Bureau of Intelligence and Research
Federal Bureau of Investigation
Cyber Threat Intelligence Integration Center

(U) This product was approved for publication by the National Intelligence Council.

UNCLASSIFIED

[redacted]

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

NATIONAL INTELLIGENCE COUNCIL

[redacted]

[redacted]

For the President
14 September 2016

[redacted]

Cyber Threats to US Election Unlikely To Alter Voting Outcomes

We assess that foreign adversaries do not have the capability to covertly overturn the vote outcome of the coming US presidential election by executing cyber attacks on election infrastructure. These adversaries—most notably Russia—can conduct cyber operations against election infrastructure to undermine the credibility of the process and weaken the perceived legitimacy of the winning candidate. Nonstate actors, such as cyber criminals and criminal hackers, also could target election infrastructure to steal data or interrupt election processes.

- Multiple checks and redundancies in the voting system make it likely that officials could detect a large-scale manipulation of election systems intended to change an outcome, especially in a well-covered US presidential election. More limited cyber operations manipulating vote counts at a small scale may be possible, potentially through physical or close-access operations. Adversaries also can use remote access to affect other parts of US election infrastructure, including voter registration records.

- We assess that Russia has increased the aggressiveness of cyber capabilities used against US Government and political targets as demonstrated by recent high-profile operations against a national political party. The Kremlin probably has intended for these operations in part to undermine public confidence and call into question the legitimacy of the US political process.

- Adversaries may use international media to spread information that they believe damages public confidence in the security of election-related networks. During Ukraine's presidential election in 2014, hackers with probable ties to Russian intelligence conducted cyber operations that included attempts to post a chart depicting a fake winner on the Central Election Commission's website—the fake winner later was broadcast through Russian media—probably with the intent to undermine voter confidence.

We assess that cyber criminals and criminal hackers probably will attempt to steal sensitive personal data and conduct cyber operations—such as denial-of-service attacks or web defacements—against public election-related websites to disrupt elections in the lead-up to, and potentially during, voting.

- Voter registration databases in Arizona and Illinois were compromised by unknown cyber actors in June and July, respectively, according to the FBI and an organization supporting cyber security in state governments. No tampering with records was indicated, and only in Illinois was theft confirmed. We have no current evidence of similar compromises, despite observed scanning for common vulnerabilities and use of unsophisticated tactics against voter-related websites in at least three other states.

Continued . . .

[redacted]

- Nonstate cyber actors probably have the capability and intent to steal voter registration data, based on similarities with past operations targeting bulk personally identifiable information.

- Although we assess that theft—not designed to disrupt or alter voting processes—is the most likely cyber criminal threat to US election infrastructure, compromises of voter registration databases and election-related networks could provide capable state actors the access needed to manipulate or disrupt operations.

Prepared by DHS with reporting from CIA, DHS, FBI, NSA, OSE, State, and open sources.

[redacted]

[redacted] Vulnerability of Computer-Enabled Election Systems to Manipulation

[redacted] [redacted]

	VULNERABILITY TO MANIPULATION	DOMESTIC EXAMPLE OF RISK
Electronic voting systems	Electronic voting systems that do not provide a paper audit trail would provide the best opportunity for covertly manipulating the outcome of an election. However, they are usually not directly connected to the Internet and would require resource-intensive supply chain, insider-enabled, or close-access operations to misregister votes or disrupt voting on a large scale.	Counties and parishes in 16 states employ electronic voting systems without a paper audit trail, although many of those jurisdictions employ other forms of voting as well. About 61.5 million registered voters vote in those jurisdictions.
Voter records	Cyber actors could delete, manipulate, or deny access to voter records to selectively suppress voting; however, backup records can mitigate effects of such activity if manipulation is detected before voting starts.	States employ three methods of maintaining voter registration databases: managed by the state, managed by localities, or hybrid. State-managed systems have greater potential for larger scale manipulation because of the centralization of records; however, state-level cyber security is often better than that of localities. A recent compromise of state voter registration systems indicates theft of data, rather than manipulation of records.
Online ballot returns	These are often restricted to overseas citizens and are therefore limited in terms of scalability, but their online nature puts them at more risk than other computer-enabled parts of the election system.	Alaska allows all voters to submit an absentee ballot electronically; 24 additional states and the District of Columbia allow voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) to submit ballots using e-mail or Internet portal. DoD projects that 154,000 UOCAVA votes—0.1 percent of ballots cast in 2012—will be submitted electronically this year.

[redacted] [redacted]

	VULNERABILITY TO MANIPULATION	DOMESTIC EXAMPLE OF RISK
Local or state compilation	Computer-enabled systems to tabulate votes recorded on paper-based ballots are often used to count votes at the local level.	Almost every county in the US uses some type of computer-enabled tabulation. Officials can recount by hand if verification checks suggest discrepancies in the tabulation process. In some cases, however, recounting by hand is not possible, such as when ballots are destroyed after initial optical scans or when paperless electronic voting machines are used.
Transmission to county or state election authorities	Denial-of-service attacks or other disruptive operations could temporarily disrupt online transmission of vote results, but officials could use alternative means to share them, such as telephonically. In addition, network-enabled systems that aggregate votes at the local, county, or state level are potentially vulnerable to manipulation, but discrepancies between tallies increase the likelihood that any large-scale manipulation would be exposed.	Most states rely on public telecommunications infrastructure to transmit vote results, although some have dedicated infrastructure that can be used. Centralized locations tabulating multiple precincts' votes provide opportunities for larger scale vote manipulation. Some states are using cloud services—online infrastructure purchased from private-sector providers—to transmit results and count and log vote.
Public dissemination of voting results	Although government or media websites featuring national vote tallies are relatively accessible, election authorities would notice the discrepancy and correct it quickly.	Each state employs its own vote reporting system, generally called an Election Night Reporting System. These systems can be vendor-provided solutions or developed by a state. Many states use cloud services to host results on election night because of the significant demand during that period.

From: [redacted]-DNI-
Sent: Wednesday, December 07, 2016 2:09 PM
To: [redacted]
Cc: [redacted]; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-
Subject: ACTION: NIOs - DNI TPs for 12/9 Restricted PC on Russia-Cyber - Due 1500 Thursday
Attachments: Tab B - 2016-22827-IC_PDBCyberActivityAgainstUSElections_DHSv2_clean.docx

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
=====================================================
```

All,

With the PC having moved to Friday morning, please send me proposed TPs and Scenesetter by 1500 on Thursday. Thank you.

Separately, for everyone's reference, below are the revised TPs that the DNI mentioned at the backbrief yesterday. What I did was lift key lines from the draft PDB that is attached.

[redacted]

ACTIVITY ON AND SINCE ELECTION DAY

[redacted] We assess that foreign adversaries did not use cyber attacks on election infrastructure to alter the US Presidential election outcome this year.

- We have no evidence of cyber manipulation of election infrastructure intended to alter results.

- There was, however, minimal targeting of election infrastructure probably by cyber criminals to steal data, although these efforts did not disrupt the election.

  - Unattributed denial-of-service attacks against election infrastructure were reported on election day, including a 4-minute attack against an unspecified Illinois elections website that had no impact on the website's availability.

[redacted] Since the election, cyber actors linked by signals intelligence to Russia's SVR on 9 November conducted multiple election-themed spear-phishing campaigns.

- Large quantities of emails – purportedly Clinton Foundation election postmortems from a Harvard University email address – were sent to individuals in national security, defense, international affairs, public policy, and European Asian studies organizations. Multiple US Government agencies report having received the emails.

OTHER INTRUSIONS

[redacted] Prior to the election, there were two reported instances of compromises against state election networks (Arizona and Illinois) and 20 or more states reported experience vulnerability scanning attempts and attempts to compromise web sites, which in most cases originated from servers operated by a Russian company.

- We now assess with low-to-moderate confidence that Russian Government-affiliated actors compromised the Illinois voter registration database and tried to compromise comparable infrastructure in multiple other states.

- We assess that a probable criminal cyber actor targeted the voter database in Arizona, based on the fact that a known criminal posted credentials for the database online.

DNC INTRUSION

[redacted] The US Intelligence Community has high confidence in its attribution of the intrusions into the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC) networks, based on the forensic evidence identified by a private cyber-firm and the IC's review and understanding of cyber activities by the Russian Government.

[redacted] Most IC agencies assess with moderate confidence that Russian services probably orchestrated at least some of the disclosures of US political information. Our level of confidence is based on the timing and that Russian intelligence was in possession of leaked information from both the DNC and DCCC as was subsequently leaked by Guccifer 2.0, the WikiLeaks website, and the DCLeaks website. In addition, the disclosures of White House e-mails by the DCLeaks website appear to be consistent with the tactics and motivations of the Russian Government.

[redacted]

From: [redacted]-DNI-
Sent: Saturday, December 03, 2016 9:21 PM
To: [redacted]
Cc: [redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted];
[redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]

[redacted]
Subject: ACTION: NIOs - DNI TPs for 12/7 Restricted PC on Russia-Cyber

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
=======================================================
```

NIOs,

I expect the DNI will attend the Russia-Cyber Restricted PC on 12/7. Will you please send me the TPs and Scenesetter for the DNI by 1400 on Tuesday (12/6)?

Thank you.

[redacted]

```
=======================================================
Classification: [redacted]

=======================================================
Classification: [redacted]
```

Pulled December PDB draft

For the President
8 December 2016

Cyber Manipulation Of US Election Infrastructure To Remain A Challenge

We assess that Russian and criminal actors did not impact recent US election results by conducting malicious cyber activities against election infrastructure. Russian Government–affiliated actors most likely compromised an Illinois voter registration database and unsuccessfully attempted the same in other states. Election monitoring and the type of systems targeted—infrastructure not used to cast or count votes—make it highly unlikely it would have resulted in altering any state's official vote result. Criminal activity also failed to reach the scale and sophistication necessary to change election outcomes. New election technology in the future that decreases diversity in systems and expands computer-enabled functions provides additional avenues to manipulate votes, but it will remain a significant challenge to sway elections through cyber means.

- Possible Russian Government–affiliated cyber actors extracted voter data, mostly containing names and addresses of voters, from Illinois's Board of Elections registration database in July that lacked adequate security safeguards. We also observed scanning and similar efforts against Secretary of State systems and websites in up to 20 more states from servers operated by a Russian-owned company with ties to Russian military cyber actors—the same infrastructure used against Illinois.[redacted] [redacted]
[redacted] [redacted]

- We have low-to-moderate confidence in the Russian Government's involvement because of our uncertainty about its utility for a state actor, a lack of observed effects from the low-profile operation, and the actors' use of obfuscation techniques, which included substantial overlap with criminal actors using similar targeting patterns and tactics. The activities did coincide with high-profile Russian cyber-enabled data leaks during the election, which we assess probably were intended to cause psychological effects, such as undermining the credibility of the election process and candidates.[redacted]

For profit cyber criminals and criminal hackers tried to steal data and to interrupt election processes by targeting election infrastructure, but these actions did not achieve a notable disruptive effect. Several technical issues with computer-enabled infrastructure were also reported, but they probably were routine software or hardware malfunctions—such as the use of old electronic voter rolls in North Carolina and technical difficulties with electronic voting machines in Pennsylvania and Utah—and were not the result of malicious activity. [redacted]

- We assess that a probable criminal cyber actor targeted a voter database in Arizona in April, using e-mail phishing to steal a single set of administrative credentials for the system—credentials that were later used to access the system in June and were posted online by a known criminal cyber actor who collects personally identifiable information. [redacted]

- On 8 November, a cybercriminal actor posted screenshots of information on Twitter resembling voting results from Alaska's state elections website and claimed to have administrative access to the website. The actor's successful but fraudulent access was resolved that day and there is no evidence of altered voting results; however, the FBI continues to investigate the incident. [redacted]

- Unattributed distributed denial of service attacks against election infrastructure were reported on election day, including a 4-minute attack against an unspecified Illinois elections website. That attack had no impact on the website's availability, according to information from Illinois' state fusion center. [redacted] In addition, a US cyber security company observed distributed denial of service attacks on the same day directed against websites associated with the US election and press systems; however, we have no reporting of how these websites were impacted. [redacted]

We assess that US election infrastructure will remain a target of growing interest for both foreign adversaries and nonstate actors during the next four years, with designs for compromise of election-related networks, theft of data, as well as disruptive and potentially manipulative activities enabled by cyber means. We assess that actors intent on covertly altering vote outcomes would, at least in part, target electronic voting machines to achieve such goals. The most likely cyber operations will probably continue to be those designed to steal data or disrupt electoral processes.

- We judge that Russia, China, Iran, and North Korea will have the ability to steal data from election-related networks, as well as execute a variety of disruptive attacks and even data manipulation on some election infrastructure. [redacted]

[redacted] We assess foreign adversaries will likely weigh the risk of appearing to influence US elections if caught or implicated, relative to any perceived benefit.

- We assess that the introduction of new technologies in the voting process will increase vulnerabilities and decrease diversity in computer-enabled US election system in the future. These technologies include cloud-based information technology infrastructure, electronic poll-books, ballot-on-demand printers, and online voting systems. Depending on the intent and capability of a future cyber actor targeting US elections, the procurement of these new machines may present a supply-chain risk.

- Moves to create additional Internet connections to election infrastructure responsible for casting and officially counting votes could provide more vulnerability to foreign adversaries and nonstate actors. Increases in the online submission of ballots, such as in Alaska where absentee ballots are allowed through an Internet portal, provides avenues for disruptive and manipulative operations. Cyber actors could attempt a denial of service attack to prevent upload of ballots, redirect would-be voters to non-existent or fraudulent websites, or attempt to manipulate the vote through compromise of voting servers.

- Persistent difficulties anticipating decisive tipping points in a nation-wide contest, as well as the decentralized nature of the systems and the election process, will continue to limit the effectiveness of cyber operations intended to alter an outcome. However, a lack of centralized standards for voter registration and voting systems provides an opportunity to improve computer network defenses. Outreach to elections officials on security assessments and cyber defense best practices, as well as engagement with private sector companies that develop and provision election infrastructure, would likely inhibit actors' ability to compromise systems and stymie further operations.

Prepared by DHS with reporting from CIA, DIA, DHS, FBI, NSA, State, and open sources.

[redacted]

Background Note for: Cyber Manipulation Of US Election Infrastructure To Remain A Challenge ([redacted])

Contact Information: Author: [redacted], DHS/I&A, [redacted] Supervisor: [redacted], DHS/I&A, [redacted]

Why are we writing this article now? This piece will build upon our previous 14 September PDB by providing assessments on observed cyber activity against US elections up until 8 November. While there were notably more high-profile cyber operations surrounding this election cycle, this piece discusses election infrastructure specifically and what we observed.

What is the US policy context for this story? This PDB is in support of the administration's consideration of US election systems as critical infrastructure and NSC efforts to identify cyber risk in the US election system. This article also provides a nuanced perspective on what occurred as a potential harbinger for future cyber threats to US elections, which can shape mitigation and outreach efforts going forward.

What are one or two key takeaways from this article? We have low-to-moderate confidence that Russian government-affiliated actors used common tactics to successfully compromise an Illinois voter registration database and used similar infrastructure and tools to unsuccessfully engage comparable infrastructure in multiple other states. Probable cyber criminals and hacktivists also likely participated in low-level targeting of election infrastructure to attempt theft of data and to interrupt election processes, although those efforts did not achieve a notable effect.

With whom on the NSC staff did you discuss this article? The Special Assistant to the President and Cybersecurity Coordinator, Michael Daniel, and multiple cybersecurity directors were briefed prior to the election on threats to election infrastructure. This piece will build on that previous analysis and the 14 September PDB on the subject.

Dissemination Restrictions: None

Source Note and Intel Gaps: The assessments about vulnerabilities in computer-enabled election systems is drawn from open sources, DHS' Office of Cyber and Infrastructure Analysis, knowledge of outreach efforts to state and local officials in the lead-up to the election, along with information from a NIC-sponsored conference. We have moderate confidence in our assessments about these vulnerabilities because of the diversity in how voting districts integrate computer-enabled technology and the systems used to identify and correct problems during the voting process. We have less confidence in attribution of Russian presence on state-level election infrastructure [redacted]

Previous PDB Items: PDB Article: Cyber Threats to US Election Unlikely To Alter Voting Outcomes (14 September 2016); [redacted]

[redacted]

[redacted]

Explanatory Qs and As:

[redacted] ***How do you define computer-enabled election systems/infrastructure?***

[redacted] We use the term election system/infrastructure in this PDB to refer to the voting process, including: registering to vote; casting ballots; tabulating votes; transmitting votes from precinct and local districts to state authorities; and publicly disseminating the final vote totals. Computer-enabled technologies like voter record databases and electronic voting machines have been integrated into the process in many states and precincts, but less technological methods like mail-in voter registration and paper ballots still are widely used as well.

[redacted] ***What kind of checks and redundancies exist in the voting system and how might they be avoided through cyber means?***

(U/[redacted]) Multiple checks and redundancies exist in US election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaigns and election officials to check, audit, and validate results. Based on analysis conducted by DHS' Office of Cyber and Infrastructure Analysis, which incorporated numerous interviews with state and local officials and private cybersecurity experts, successfully mounting widespread cyber operations against US voting machines, enough to affect a national election would require a multiyear effort with significant human and information technology resources available only to a nation-state. The level of effort and scale required to change the outcome of a national election, however, would make it nearly impossible to avoid detection. This risk analysis is based on the diversity of systems, the need for physical access to compromise voting machines, and the security and pre-election testing employed by state and local officials. In addition, the vast majority of localities engage in logic and accuracy testing, which work to ensure voting machines operate and tabulate as expected before, during, and after the election.[redacted] [redacted] ***How vulnerable are electronic voting machines to manipulation?***

[redacted] If an adversary is able to gain access to an electronic voting machine, poor computer security measures associated with most electronic voting machines leave them highly vulnerable to manipulation. Many electronic voting machines used in the presidential election this year were at least 10 years old and contain hardware, software, and firmware that are likely defenseless to computer viruses and malware and often are stored unattended for a significant period of time with minimal security measures in polling locations, potentially making them more accessible to third party manipulation. However, gaining access to electronic voting machines generally would require resource-intensive supply chain operations, physical or close access, or an insider. This would very likely be detected due to a

[a] (U) Voting precincts in more than 3,100 counties across the United States use nearly 50 different types of voting machines produced by 14 different manufacturers. The diversity in voting systems and versions of voting software provides significant security by complicating attack planning. Most voting machines do not have active connections to the Internet. The vast majority of localities engage in logic and accuracy testing, which work to ensure voting machines operate and tabulate as expected before, during, and after the election.

substantial personnel effort across all voting places that the malicious actors wish to impact. If this was done on a wide scale and resulted in lopsided results well outside previous voting norms for the voting places in question, public polling, and exit polls, then indirect evidence of tampering would very likely be apparent. However, if the manipulated results fell near predicted results, then it would be more difficult to statisticians, the media, and others to detect. Electronic voting machines are usually not directly connected to the Internet, but patches, system updates and ballot definition files transferred via or stored on networks accessible to the Internet also create the potential to remotely insert malicious software.[redacted]

[redacted] ***How widely used are electronic voting machines in the US?***

[redacted] Many states and localities have been moving away from the paperless electronic voting machines that are the most vulnerable to covert manipulation. Electronic voting machines with no paper verification currently are the primary voting method in five states (Delaware, Georgia, Louisiana, New Jersey, and South Carolina), and are used in combination with paper-verified electronic voting machines and/or paper ballots in an additional ten according to a nonprofit US voter verification organization. Three states use mail-in ballots, and the remaining states use electronic voting machines with a paper trail and/or paper ballots that may be scanned and tabulated with computer-enabled equipment.

[redacted] ***What redundancies are built into the election system to prevent accidental miscounts or fraud?***

[redacted] Votes are initially tabulated at the local level, where paper ballots, optical scan sheets and electronic voting machines that provide a paper record provide election officials a way to recount ballots by hand in the case of a contested election. In localities with robust verification requirements, checks such as random audits of voting equipment to make sure it is counting correctly or verifying that the number of votes cast in a precinct does not exceed the number of registered voters help to catch accidental or intentional miscounts. Once votes are tabulated at the precinct or county level, discrepancies that emerge as results are tabulated at the state level are relatively obvious. In addition to government safeguards, the media, political party poll watchers, and nongovernment organizations closely track election results in key districts.

[redacted] ***How could adversaries have identified which states or local voting districts would have the most impact?***

[redacted] Media organizations, polling companies, and think tanks that tracked voter sentiment in the runup to the election provide a wealth of publicly available data that foreign adversaries could have used to narrow in on swing states or key precincts where vote manipulation could have the biggest impact. In addition, foreign adversaries could have used data obtained via computer intrusions, such as data from the networks of candidate campaigns and political parties, to research which states or precincts they think are the most crucial.

[redacted] ***How was the IC positioning to monitor threats to US computer-enabled election systems?***

[redacted] DHS monitored reported incidents and established a working group to conduct an outreach campaign to state/local authorities focusing on the cybersecurity of the US's voting infrastructure, to include protecting voter registration databases and electronic and Internet voting. A Cyber Unified Coordination Group (UCG), led by DHS, FBI, and ODNI/CTIIC was formed to monitor and respond to any potential incident. FBI's Cyber Action Team was prepared to deploy and assist local government or private industry that identified a need for technical personnel.

[redacted] ***What underlies our attribution of the Illinois incident (and similar activity in other states) to Russian government-affiliated cyber actors?***

[redacted] The low-to-moderate assessment that Russian government-affiliated cyber actors were responsible largely is based on analysis of the infrastructure used against the Illinois network—mostly operated by Russia-based King Servers, which has been tied to suspected Russian military cyber actors that leased infrastructure from King Servers as early as December 2009 and communicated as recently as January 2016, [redacted] Additional infrastructure—[redacted]—tied by a private cybersecurity firm to a 2016 Russian military cyber spear-phishing campaign against an Eastern European government was also discovered in Illinois' logs.[redacted] The correlation to up to 20 further states is based on use of the same infrastructure, the same specific vulnerability, as well as similarities in the concurrently targeted election-related networks of those other states.

[redacted] ***What limits our confidence in the attribution of the Illinois incident to Russian government-affiliated cyber actors?***

[redacted] Our low-to-moderate confidence level [redacted] The activity against state-run election infrastructure—largely unsuccessful in compromise and relatively low-level in detectability—is notable in its operational differences with the high-profile and concurrent Russian cyber-enabled data leaks. Although we continue to assess the data leaks probably were intended to produce psychological pressure, we have not identified a clear intent for these notably different operations against election infrastructure. Additionally, some of the infrastructure used against Illinois has been used in The Onion Router (TOR)—a network designed to conceal identities and activity—[redacted]

[redacted]

From: [redacted]-DNI-
Sent: Thursday, December 08, 2016 8:32 AM
To: [redacted] DHS USA GOV; [redacted]-DNI-; [redacted]; [redacted] DHS USA GOV
Cc: [redacted]-DNI-; [redacted]-DNI-; [redacted]; [redacted]-DNI-
Subject: RE: [redacted] FW: Election PDB

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted]

For clarification [redacted], the ICA probably won't be done until mid-January. We are tentatively shooting for 9 January to send a possibly draft, possibly final, version to POTUS. We are hoping for final agreement on scope/length/classification to come out of a PC on Friday.

The room's thoughts (EEMC, NIO Russia, CTIIC, NSA, FBI, CCI) were that it was worth going ahead with the pdb if possible now to provide our current understanding of what happened during the election, and that worst case the ICA has some language and an associated briefer note explaining any changes between the products.

It is OK if you really need to run them simultaneously, but recognize this is an issue of high level of congressional and WH interest right now, and to do below would postpone its publication for a month.

[redacted]

[redacted]
Deputy National Intelligence Officer for Cyber Issues
[redacted]

-----Original Message-----
From: Wright, Christopher J. [mailto:[redacted]dhs[redacted]
Sent: Wednesday, December 07, 2016 4:10 PM
To: [redacted]-DNI-[redacted]@dni[redacted]; Sohnia A. Azim
[redacted]@cia[redacted]; [redacted] DHS USA GOV [redacted]@dhs[redacted]
Cc: [redacted]-DNI-[redacted]@dn[redacted]; [redacted]-DNI-
[redacted]@dni[redacted]; [redacted]-DNI-[redacted]@dni[redacted]

Subject: RE: [redacted] FW: Election PDB --- [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

+NIO Cyber

[redacted], thanks. We'll follow the coordination [redacted] process spelled out below. Roger on the balancing act, which I think we did fairly adeptly last time.

[redacted], recognize you're shorthanded over there this week. Let us know if/how we can provide a jump start. We previously worked mostly through [redacted] and [redacted] (CIA). Depending on the specifics of the tasking, perhaps [redacted] is our better counterpart. Standing by to help.

[redacted]

[redacted]

Chief, NCCIC Intelligence Support Branch
DHS Office of Intelligence & Analysis (I&A)
[redacted]
[redacted] @hq.dhs. [redacted]
[redacted] @dhs. [redacted]
[redacted] @dhs. [redacted]

-----Original Message-----
From: [redacted] -DNI- [mailto: [redacted] @dn [redacted]
Sent: Wednesday, December 07, 2016 4:05 PM
To: [redacted]; [redacted]; [redacted]
Subject: RE: [redacted] FW: Election PDB

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted]

I'm ok with that. As with last time, we will probably send out the ICA and the PDB near same time to make sure they have the same bottom lines. That was a bit of a balancing act previously.

[redacted]

[redacted]
Deputy Director / PDB / ODNI
[redacted]
[redacted]@dni[redacted]

-----Original Message-----
From: [redacted] [mailto[redacted]@dhs[redacted]
Sent: Wednesday, December 07, 2016 3:53 PM
To: [redacted]@cia[redacted]; [redacted] DHS USA GOV
[redacted]@dhs.[redacted]
Cc: [redacted]-DNI-[redacted]@dni[redacted]
Subject: RE: [redacted] FW: Election PDB --- [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==

[redacted]
We spoke with the NIO Cyber shop, who discussed the prospect of a NIC product in response to POTUS at their afternoon (1400) session. They agreed that it would still be worth running a separate and earlier PDB and including in the BN that a more comprehensive product is forthcoming. This would mirror our PDB and the ICA that were produced in early September. We'll obviously be supporting their product in the same way.

Regarding [redacted] we have some issues with getting an additional person or two read-in, but we agree that it should be addressed in the paper and will work to do that soonest, with a nod to the more specific information. Given the classification level and that it wouldn't change the analytic line, we thought it worthwhile to try and re-coordinate soonest with a [REDACTED] tick that we would craft concurrently.

Does that sound like a viable pathway?

V/r,
[redacted]

[redacted]

Chief, NCCIC Intelligence Support Branch
DHS Office of Intelligence & Analysis (I&A)

[redacted]
[redacted]@hq.dhs[redacted]
[redacted]@dhs.[redacted]
[redacted]@[redacted]

-----Original Message-----
From: [redacted]@cia[redacted]
Sent: Wednesday, December 07, 2016 3:41 PM
To: [redacted]
Cc: [redacted]-DNI-; [redacted]
Subject: RE: [redacted] FW: Election PDB

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==

[redacted]

Just tried calling you. Did you see [redacted] email to you?

[redacted]
PDB Editor
Secure: [redacted]
[redacted]@cia.[redacted]

-----Original Message-----
From: [redacted] [mailto:[redacted]@dhs[redacted]
Sent: Wednesday, December 07, 2016 3:33 PM
To: [redacted]@cia[redacted]
Cc: [redacted]-DNI- <[redacted]@dni[redacted]; [redacted] DHS
USA GOV [redacted]@dhs[redacted]
Subject: FW: [redacted] FW: Election PDB --- [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==

Hi [redacted]

Good afternoon! This email is what my question is related to - if PASS is ok with this PDB going forward, and possibly including in the BN mention of the

POTUS NIC tasking. Please let me know if you have any questions.

Thanks,

[redacted]
NCCIC Intelligence Support Branch
Cyber Division
DHS Office of Intelligence & Analysis
JWICS: [redacted]@dhs[redacted]
SIPR:[redacted]@dhs[redacted]
UNCLASS: [redacted]@hq.dhs[redacted]
[redacted]

-----Original Message-----
From: [redacted]-DNI-[redacted]
Sent: Wednesday, December 07, 2016 3:19 PM
To: [redacted]; [redacted]
Cc: [redacted]; [redacted]-DNI-
Subject: RE: [redacted] FW: Election PDB

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]

==

[redacted]

In discussion at the 2:00 people seemed to agree it is worth still running the pdb if PASS is interested with something being included in the background note to highlight the POTUS tasking and that this pdb is an interim step while we work on the more comprehensive task.

[redacted]

[redacted]
Deputy National Intelligence Officer for Cyber Issues
[redacted]

==
Classification: [redacted]

==
Classification: [redacted]

==
Classification: [redacted]

==
Classification: [redacted]

==
Classification: [redacted]

==
Classification: [redacted]

From: [redacted] (FBI) [redacted]
Sent: Thursday, December 08, 2016 4:47 PM
To: [redacted] dhs [redacted] ; [redacted] FBI [redacted] ; [redacted] DHS [redacted] ; [redacted] -DNI-; [redacted] ; [redacted] -DNI-; [redacted] DHS [redacted] ; [redacted] DHS [redacted] ; [redacted] DHS [redacted] ; [redacted] FBI [redacted] ; [redacted] DHS [redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted] ; [redacted] DIA [redacted] ; [redacted] ; [redacted] FBI [redacted] ; [redacted] ; [redacted] DHS [redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted] ; [redacted] STATE [redacted] ; [redacted] STATE [redacted] ; [redacted] DIA [redacted] ; [redacted] NGA [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] DIA [redacted] ; [redacted] NSA- [redacted] ; [redacted] -DNI-; [redacted] -DNI-; [redacted] -DNI-; [redacted] ; [redacted] FBI [redacted] ; [redacted] DHS [redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted] ; [redacted] STATE [redacted] ; [redacted] STATE [redacted] ; [redacted] DIA [redacted] ; [redacted] NGA [redacted] ; [redacted] DIA [redacted] ; [redacted] NSA- [redacted] -DNI-; [redacted] -DNI-; [redacted] -DNI-; [redacted] ; [redacted] -DNI-; [redacted] -DNI-; [redacted] ; [redacted] DHS [redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted] ; [redacted] DIA [redacted] ; [redacted] NSA- [redacted] ; [redacted] FBI [redacted] ; [redacted] ; [redacted] DHS [redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted] ; [redacted] STATE [redacted] ; [redacted] STATE [redacted] ; [redacted] DIA [redacted] ; [redacted] NGA [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] DIA [redacted] ; [redacted] NSA- [redacted] -DNI-; [redacted] -DNI-; [redacted] -DNI-; [redacted] ; [redacted] FBI [redacted] ; [redacted] DHS [redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted] ; [redacted] STATE [redacted] ; [redacted] STATE [redacted] ; [redacted] DIA [redacted] ; [redacted] NGA [redacted] ; [redacted] DIA [redacted] ; [redacted] NSA- [redacted] ; [redacted] -DNI-; [redacted] -DNI-; [redacted] -DNI-; [redacted] ; [redacted] -DNI-; [redacted] -DNI-; [redacted] ; [redacted] DHS [redacted] ; [redacted] DHS [redacted] ; [redacted] DHS [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] DHS [redacted] ; [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] -DNI-; [redacted] DHS [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted] ; [redacted] FBI [redacted]
Cc: [redacted] DHS [redacted] ; [redacted] dhs [redacted] ; [redacted] DHS [redacted] ; [redacted] DHS [redacted] ; [redacted] -DNI-; [redacted] -DNI-; [redacted] ; [redacted] ; [redacted] ; [redacted] ; [redacted] ; [redacted] ; [redacted] ; [redacted] ; [redacted] ;

Cc: [redacted]; [redacted] FBI [redacted]
Subject: RE: [redacted] PDB Coordination Request - COB 8 December --- [redacted]
[redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

Thanks for sending the revision, we will take a closer look at it tomorrow.

[redacted]

____
[redacted]
Supervisory Intelligence Analyst
FBI Cyber Division
Eurasia Cyber Intelligence Unit
[redacted]

-----Original Message-----
From: [redacted] DHS[redacted]
Sent: Thursday, December 08, 2016 4:32 PM
To: [redacted] (FBI); [redacted]; [redacted] -DNI-; [redacted] -DNI-; [redacted] -DNI-;
[redacted]; [redacted]; [redacted] (FBI); [redacted]; [redacted]
[redacted]; [redacted] NSA- [redacted]; [redacted] DIA [redacted]; [redacted]
[redacted]; [redacted] (FBI); [redacted]; [redacted]; [redacted] NSA- [redacted]
[redacted] NSA- [redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted]
[redacted] DIA [redacted]; [redacted] NGA [redacted]; [redacted] (FBI); [redacted]
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted]
[redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]; [redacted] (FBI);
[redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]; [redacted] STATE
[redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]
[redacted]; [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted]
[redacted] -DNI-'; [redacted] -DNI-'; [redacted]; 'Cc: [redacted] -DNI-'; ' [redacted] -DNI-'; ' [redacted]
[redacted] -DNI-'; [redacted]; [redacted] NSA- [redacted] '; [redacted] NSA- [redacted] '; [redacted]
[redacted] DIA [redacted] '; [redacted] NSA- [redacted] '; [redacted] (FBI); [redacted];
[redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]; [redacted] STATE
[redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]
[redacted]; [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] DIA [redacted];
[redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]
[redacted]; [redacted] (FBI); [redacted]; [redacted] NSA- [redacted]; [redacted]
[redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted];
[redacted] NGA [redacted]; [redacted] DIA [redacted]; [redacted] NSA- [redacted];
[redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]; 'Cc: [redacted] -
DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]; [redacted]; [redacted]; [redacted]

[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted]; [redacted]; [redacted] (FBI); [redacted]
(FBI); [redacted] -DNI-; [redacted]; [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted] (FBI)
Cc: [redacted]; [redacted]; [redacted]; [redacted]; [redacted] -DNI-; [redacted]
[redacted] -DNI-; [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; [redacted];
[redacted]; [redacted]; [redacted]; [redacted]; [redacted]; [redacted] (FBI)
Subject: RE: [redacted] PDB Coordination Request - COB 8 December --- [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==

Until receiving the email below, the only difference that I was aware of between FBI and I&A over this transparently developed product was over confidence level on the attribution, which we have adjusted (to the FBI's view) upon review of the recent redacted [redacted] collection. Rather than drafting a dissent, perhaps FBI could share their concerns with the most recent draft (attached). I think it goes without saying that this PDB should not go forward until the FBI has done so.

-----Original Message-----
From: [redacted] (FBI) [redacted]
Sent: Thursday, December 08, 2016 3:48 PM
To: [redacted]; [redacted] -DNI-; [redacted] -DNI-; [redacted] -DNI-; [redacted]; [redacted]
[redacted]; [redacted]; [redacted] (FBI); [redacted]; [redacted] NSA- [redacted]; [redacted]
[redacted] NSA- [redacted]; [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted]
(FBI); [redacted]; [redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]
[redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted];
[redacted] NGA [redacted]; [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted] -DNI-
'; [redacted] -DNI-'; [redacted]; [redacted] (FBI); [redacted]; [redacted] NSA-
[redacted]; [redacted] NSA- [redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]
[redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]; [redacted] DIA [redacted]
[redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-
'; [redacted]; 'Cc: [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]; [redacted]
[redacted] NSA- [redacted]; [redacted] NSA- [redacted]; [redacted] DIA [redacted]; [redacted]
[redacted] NSA- [redacted]; [redacted] (FBI); [redacted]; [redacted]; [redacted]
[redacted]; [redacted] NSA- [redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]
[redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]; [redacted] (FBI);
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted]
(FBI); [redacted] (FBI); [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted]
[redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]; [redacted] (FBI);
[redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]; [redacted] STATE
[redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]
[redacted]; [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted]
[redacted] -DNI-'; [redacted] -DNI-'; [redacted]; 'Cc: [redacted] -DNI-'; [redacted] -DNI-'; [redacted]
[redacted] -DNI-'; [redacted]; [redacted]; [redacted]; [redacted] (FBI); [redacted] (FBI); [redacted]

[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted]; [redacted]; [redacted] (FBI); [redacted] (FBI); [redacted] -DNI-; [redacted]
[redacted]; [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted] (FBI); [redacted]; [redacted] (FBI); [redacted] (FBI); [redacted]
(FBI)
Cc: [redacted]; [redacted]; [redacted]; [redacted]; [redacted] [redacted]
[redacted] -DNI-; [redacted] -DNI-; [redacted]; [redacted]; [redacted]; [redacted]; [redacted]
[redacted]; [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; [redacted];
[redacted] (FBI)
Subject: RE: [redacted] PDB Coordination Request - COB 8 December --- [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===
[redacted], FBI will be drafting a dissent this afternoon. Please remove our seal an annotations of co-authorship.

[redacted]

-----Original Message-----
From: [redacted] DHS [redacted]
Sent: Thursday, December 08, 2016 2:22 PM
To: [redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] DHS [redacted]; [redacted] DHS [redacted];
[redacted] DHS [redacted]; [redacted] (FBI) [redacted]; [redacted]
[redacted] DHS [redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]
[redacted]; [redacted] DIA [redacted]; [redacted]
NSA- [redacted]; [redacted] (FBI) [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] DHS [redacted]; [redacted] NSA- [redacted]
[redacted]; [redacted] NSA- [redacted]; [redacted] STATE [redacted]
[redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]
[redacted]; [redacted] NGA [redacted];
[redacted] (FBI) [redacted]; [redacted] (FBI) [redacted]; [redacted]
[redacted] (FBI) [redacted]; [redacted] (FBI) [redacted]; [redacted]
(FBI) [redacted]; [redacted] (FBI) [redacted]; [redacted] DIA [redacted]
[redacted]; [redacted] NSA- [redacted] ' [redacted] -
DNI-' [redacted]; [redacted] -DNI-' [redacted]; [redacted] -DNI-'
[redacted]; [redacted] cia. [redacted]; [redacted] (FBI) [redacted]; [redacted]
[redacted] DHS [redacted]; [redacted] NSA- [redacted]; [redacted] [redacted]
[redacted]; [redacted] STATE [redacted]; [redacted] STATE
[redacted]; [redacted] DIA [redacted]; [redacted]
[redacted] NGA [redacted]; [redacted] DIA [redacted]
[redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'
[redacted]; [redacted] -DNI-' [redacted]; [redacted] -DNI-' [redacted];
[redacted] cia [redacted] 'Cc: [redacted] -DNI-' [redacted] ' [redacted] -DNI-'
[redacted]; [redacted] -DNI-' [redacted]; [redacted] DHS [redacted]; [redacted]
[redacted] NSA- [redacted]; [redacted] NSA- [redacted];
[redacted] DIA [redacted]; [redacted] NSA- [redacted]

[redacted]; [redacted] (FBI) [redacted]; [redacted] cia [redacted];
[redacted] DHS [redacted]; [redacted] NSA- [redacted]; [redacted]
[redacted] NSA- [redacted]; [redacted] STATE [redacted]; [redacted]
[redacted] STATE [redacted]; [redacted] DIA [redacted];
[redacted] NGA [redacted]; [redacted] (FBI)
[redacted]; [redacted] (FBI) [redacted]; [redacted] (FBI)
[redacted]; [redacted] (FBI) [redacted]; [redacted] (FBI)
[redacted]; [redacted] (FBI) [redacted]; [redacted] DIA [redacted]
[redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'
[redacted]; [redacted] -DNI-' [redacted]; [redacted] -DNI-' [redacted];
[redacted] cia [redacted]; [redacted] (FBI) [redacted]; [redacted]
[redacted] DHS [redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]
[redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]
[redacted]; [redacted] DIA [redacted]; [redacted]
NGA [redacted]; [redacted] DIA [redacted]
[redacted]; [redacted] NSA- [redacted] -DNI-'
[redacted]; [redacted] -DNI-' [redacted]; [redacted] -DNI-' [redacted];
[redacted] cia [redacted]; 'Cc: [redacted] -DNI-' [redacted]; ' [redacted] -DNI-'
[redacted]; [redacted] -DNI-' [redacted]; [redacted] DHS [redacted]; [redacted]
[redacted] DHS [redacted] >; [redacted] DHS [redacted]; [redacted] (FBI)
[redacted]; [redacted] (FBI) [redacted]; [redacted] (FBI) [redacted]; [redacted]
[redacted] (FBI) [redacted]; [redacted] (FBI) [redacted]; [redacted] (FBI)
[redacted]; [redacted] (FBI) [redacted]; [redacted] (FBI)
[redacted]; [redacted] (FBI) [redacted] >; [redacted] (FBI)
[redacted]; [redacted] DHS [redacted]; [redacted] DHS [redacted]; [redacted]
[redacted] (FBI) [redacted]; [redacted] (FBI) [redacted]; [redacted] (FBI)
[redacted]; [redacted] -DNI- [redacted]; [redacted] DHS [redacted]
Cc: [redacted] DHS [redacted]; [redacted] DHS [redacted]; [redacted]
[redacted] DHS [redacted]; [redacted] DHS [redacted]; [redacted] DHS [redacted]; [redacted]
[redacted] -DNI- [redacted] -DNI- [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] cia [redacted]
Subject: RE: [redacted] PDB Coordination Request - COB 8 December --- [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==

We have so far received responses from FBI, CIA/NIC, and NGA. Please provide coordination responses ASAP if you have not been able to yet. Thank you for understanding and trying to accommodate this short coordination period, to accommodate the Administration's request for this to run tomorrow.

Thank you,

[redacted]
NCCIC Intelligence Support Branch
Cyber Division
DHS Office of Intelligence & Analysis
[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, December 08, 2016 12:59 PM
To: [redacted]-DNI-'; [redacted]-DNI-'; [redacted]-DNI-'; [redacted]; [redacted]; [redacted]
[redacted]; [redacted] FBI [redacted]; [redacted]; [redacted] NSA-[redacted]; [redacted] NSA-[redacted]
[redacted]; [redacted] DIA [redacted]; [redacted] NSA-[redacted]; [redacted] FBI [redacted]; [redacted]
[redacted]; [redacted]; [redacted] NSA-[redacted]; [redacted] NSA-[redacted]; [redacted]
[redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA
[redacted]; [redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)';
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)'; [redacted]
DIA [redacted]; [redacted] NSA-[redacted]; [redacted]-DNI-'; [redacted]-DNI-'; [redacted]
[redacted]-DNI-'; [redacted]'; [redacted] FBI [redacted] NSA-[redacted];
[redacted] NSA-[redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted]
[redacted] DIA [redacted]; [redacted] NGA [redacted] DIA [redacted];
[redacted] NSA-[redacted]; [redacted]-DNI-'; [redacted]-DNI-'; [redacted]-DNI-'; [redacted]
[redacted]; 'Cc: [redacted]-DNI-'; [redacted]-DNI-'; [redacted]-DNI-'; [redacted]; [redacted]
NSA-[redacted]; [redacted] NSA-[redacted]'; [redacted] DIA [redacted]'; [redacted]
NSA-[redacted] FBI [redacted]'; [redacted] NSA-[redacted]
[redacted]; [redacted] NSA-[redacted]'; [redacted] STATE [redacted]'; [redacted] STATE [redacted]';
[redacted] DIA [redacted]; [redacted] NGA [redacted]; [redacted] (FBI)';
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)'; [redacted]
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] DIA [redacted] NSA-[redacted];
[redacted]-DNI-'; [redacted]-DNI-'; [redacted]-DNI-'; [redacted]'; [redacted] FBI [redacted];
[redacted]; [redacted] NSA-[redacted]; [redacted] NSA-[redacted]; [redacted] STATE
[redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]
[redacted]; [redacted] DIA [redacted]; [redacted] NSA-[redacted]; [redacted]-DNI-'; [redacted]
[redacted]-DNI-'; [redacted]-DNI-'; [redacted]; 'Cc: [redacted]-DNI-'; [redacted]-DNI-'; [redacted]
[redacted]-DNI-'; [redacted]; [redacted]; [redacted]; [redacted] (FBI)'; [redacted] (FBI)';
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)';
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)'; [redacted]
[redacted] (FBI)'; [redacted]; [redacted]; [redacted] (FBI)'; [redacted] (FBI)'; [redacted]
[redacted] (FBI)'; [redacted]-DNI-'; [redacted]
Cc: [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; [redacted]
[redacted]-DNI-'; [redacted]-DNI-'
Subject: RE: [redacted] PDB Coordination Request - COB 8 December ---[redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

Hi All,

Due to high Administration interest, this piece is now scheduled to run tomorrow. Therefore, we now ask that coordination responses be sent by 2pm, so that the production process for tomorrow can be completed.

Thank you,

[redacted]
NCCIC Intelligence Support Branch
Cyber Division
DHS Office of Intelligence & Analysis
[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, December 07, 2016 4:47 PM
To: [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] ; [redacted] ; [redacted]
[redacted] ; ' FBI ; [redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted]
[redacted] ; [redacted] DIA [redacted] ; [redacted] NSA- [redacted] ; [redacted] FBI [redacted] ; [redacted]
[redacted] ; [redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted] ; [redacted]
[redacted] STATE [redacted] ; [redacted] STATE [redacted] ; [redacted] DIA [redacted] ; [redacted] NGA
[redacted] ; [redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)';
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)'; [redacted]
DIA [redacted] ; [redacted] NSA- [redacted] ; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]
[redacted] -DNI-'; [redacted] ; [redacted] FBI [redacted] ; [redacted] ; [redacted] NSA- [redacted] ;
[redacted] NSA- [redacted] ; [redacted] STATE [redacted] ; [redacted] STATE [redacted] ; [redacted]
[redacted] DIA [redacted] ; [redacted] NGA [redacted] ; [redacted] DIA [redacted] ;
[redacted] NSA- [redacted] ; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]
[redacted] ; 'Cc: [redacted] -DNI-'; ' [redacted] -DNI-'; [redacted] -DNI-'; [redacted] ; [redacted]
NSA- [redacted] '; [redacted] NSA- [redacted] ; [redacted] DIA [redacted] ; [redacted]
NSA- [redacted] ; [redacted] FBI [redacted] ; [redacted] ; [redacted] ; [redacted] NSA- [redacted]
[redacted] ; [redacted] NSA- [redacted] ; [redacted] STATE [redacted] ; [redacted] STATE [redacted] ;
[redacted] DIA [redacted] ; [redacted] NGA [redacted] ; [redacted] (FBI)';
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)'; [redacted]
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] DIA [redacted] ; ' [redacted] NSA- [redacted] ;
[redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] ; [redacted] FBI [redacted] ;
[redacted] ; [redacted] NSA- [redacted] ; [redacted] NSA- [redacted] ; [redacted] STATE
[redacted] ; [redacted] STATE [redacted] ; [redacted] DIA [redacted] ; [redacted] NGA [redacted]
[redacted] ; [redacted] DIA [redacted] ; [redacted] NSA- [redacted] ; [redacted] -DNI-'; [redacted]
[redacted] -DNI-'; [redacted] -DNI-'; [redacted] ; 'Cc: [redacted] -DNI-'; ' [redacted] -DNI-'; 'R [redacted]
[redacted] -DNI-'; [redacted] ; [redacted] ; [redacted] ; [redacted] (FBI)'; [redacted] (FBI)';
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)'; ' [redacted] (FBI)';
[redacted] (FBI)'; [redacted] (FBI)'; [redacted] (FBI)'; [redacted]
[redacted] (FBI)'; [redacted] ; [redacted] ; [redacted] (FBI); [redacted] (FBI); H [redacted]
[redacted] (FBI); [redacted] -DNI-'; [redacted]
Cc: [redacted] ; [redacted] ; [redacted] ; [redacted] ; [redacted]
Subject: [redacted] PDB Coordination Request - COB 8 December --- [redacted]

Classification: [redacted]

Classified By: [redacted]

Derived From: [redacted]
Declassify On: [redacted]
===

[redacted]

Hi All,

DHS I&A Cyber Division is requesting coordination from all recipients by COB on 8 December for this cyber/US elections PDB. If multiple colleagues from your agency are on this email (e.g., FBI) please coordinate your response within your agency so that one unified response is sent for your agency. You can send your comments back to me, and please let me know if you have any questions.

Thank you,

[redacted]
NCCIC Intelligence Support Branch
Cyber Division
DHS Office of Intelligence & Analysis
[redacted]

===
Classification: [redacted]

===
Classification: [redacted]

===
Classification: [redacted]

===
Classification: [redacted]

===
Classification: [redacted]

===
Classification: [redacted]

From: [redacted]-DNI-
Sent: Thursday, December 08, 2016 4:53 PM
To: [redacted] DHS [redacted]; [redacted]-DNI-; [redacted]; [redacted]-DNI-;
[redacted] DHS [redacted]; [redacted] DHS [redacted]; [redacted] DHS [redacted]
; [redacted] FBI [redacted]; [redacted] DHS [redacted]; [redacted] NSA- [redacted]
; [redacted] NSA- [redacted]; [redacted] DIA [redacted]
; [redacted] NSA- [redacted]; [redacted] FBI [redacted]; CIA [redacted]
; [redacted] DHS [redacted]; [redacted] NSA- [redacted]; [redacted]
[redacted]; [redacted] STATE [redacted]; [redacted]
STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA
[redacted]'; [redacted] FBI [redacted]; [redacted] FBI [redacted]; [redacted]
[redacted] FBI [redacted]; [redacted] FBI [redacted]; [redacted] FBI [redacted];
[redacted] FBI [redacted]; [redacted] DIA [redacted]'; [redacted]
[redacted] NSA- [redacted]; [redacted]-DNI-; [redacted]-DNI-; [redacted]
-DNI-; CIA [redacted]; [redacted] FBI [redacted]; [redacted] DHS [redacted]
; [redacted] NSA- [redacted]; [redacted] NSA- [redacted];
[redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted] DIA
[redacted]; [redacted] NGA [redacted]'; [redacted] DIA
[redacted]'; [redacted] NSA- [redacted]; [redacted]-DNI-; [redacted]
-DNI-; [redacted]-DNI-; CIA [redacted]; [redacted]-DNI-; [redacted]
-DNI-; [redacted]; [redacted] DHS [redacted]; [redacted] NSA- [redacted]
; [redacted] NSA- [redacted]; [redacted] DIA [redacted]
; [redacted] NSA- [redacted]; [redacted] FBI [redacted]; CIA [redacted]
; [redacted] DHS [redacted]; [redacted] NSA- [redacted] V; [redacted]
[redacted] NSA- [redacted]; [redacted] STATE [redacted]; [redacted]
STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA
[redacted]'; [redacted] FBI [redacted] [redacted] FBI [redacted]; [redacted]
[redacted] FBI [redacted]; [redacted] FBI [redacted]; [redacted] FBI [redacted]
[redacted] FBI [redacted]; [redacted] DIA [redacted]'; [redacted]
[redacted] NSA- [redacted]; [redacted]-DNI- [redacted] DNI-; T [redacted]
-DNI-; CIA [redacted]; [redacted] FBI [redacted]; [redacted] DHS [redacted]
; [redacted] NSA- [redacted]; [redacted] NSA- [redacted];
[redacted] STATE [redacted] [redacted] STATE [redacted]; [redacted] DIA
[redacted]; [redacted] NGA [redacted]'; [redacted] DIA
[redacted]'; [redacted] NSA- [redacted]; [redacted]-DNI-; [redacted]
-DNI-; [redacted]-DNI-; CIA [redacted]; [redacted]-DNI-; [redacted]
-DNI-; [redacted]; [redacted] DHS [redacted]; [redacted] DHS [redacted]
; [redacted] DHS [redacted]; [redacted] FBI [redacted]; [redacted] FBI [redacted]; [redacted]
FBI [redacted]; [redacted] FBI [redacted]; [redacted] FBI [redacted]; [redacted]
FBI [redacted]; [redacted] FBI [redacted]; [redacted] FBI [redacted] [redacted]
FBI [redacted]; [redacted] FBI [redacted]; [redacted] DHS [redacted]; [redacted]
.; [redacted] FBI [redacted]; [redacted] FBI [redacted]; [redacted] FBI [redacted];
[redacted]-DNI-; [redacted] DHS [redacted]; [redacted] FBI [redacted]
Cc: [redacted] dhs [redacted]; [redacted] DHS [redacted]; [redacted] dhs
[redacted]; [redacted] DHS [redacted] [redacted] DHS [redacted]; [redacted]
[redacted]-DNI-; [redacted]; [redacted]; [redacted]-DNI-; [redacted]
[redacted]-DNI-
Subject: RE: [redacted] PDB Coordination Request - COB 8 December

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]

==

All,

Based on some new guidance, we are going to push back publication of the PDB. It will not run tomorrow and is not likely to run until next week.

[redacted]

[redacted]
Deputy Director / PDB / ODNI
[redacted]

==

Classification: [redacted]

[redacted]

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

Summary of Conclusions for
Meeting of the Principals Committee
DATE: December 9, 2016
LOCATION: White House Situation Room
TIME: 11:30 a.m. - 1:30 p.m.

SUBJECT: Summary of Conclusions for PC Meeting on a Sensitive Topic [redacted]

Participants:

Chair
Susan Rice

OVP
No Representative

State
Secretary John Kerry (SVTS)
Victoria Nuland

Treasury
Adam Szubin

DOD
Brian McKeon

Justice
Loretta Lynch
Mary McCord

DHS
Secretary Jeh Johnson
Rob Silvers

Chief of Staff
Denis McDonough

USUN
Maher Bitar

WH Counsel
Neil Eggleston

DNI
James Clapper

FBI
Andrew McCabe

CIA
John Brennan

JCS (SVTS)
Gen Joseph Dunford

NSA
Richard Ledgett

White House
Avril Haines
Lisa Monaco
Ben Rhodes

NSC
Chris Fonzone
Caroline Tess
Brett Holmgren
Michael Daniel
Celeste Wallander
Samir Jain
Jeffrey Edmonds

[redacted]

Classified by: [redacted]
Reason: [redacted]
Declassify on: [redacted]

[redacted]

Summary of Conclusions

It was agreed that:

- Principals agreed to deny Russia the use of its residential and recreational compound at Pioneer Point on the Chesapeake Bay. Principals also recommended, pending the views of the U.S. Mission to the United Nations (USUN) and legal review, denying Russia the use of its residential and recreational compound in Glen Cove, New York. The Department of State noted its preference that any action against the compounds be delayed to, among other things, allow for a potential agreement on Aleppo to be implemented. State also will provide a matrix of possible Russian responses, both operationally and diplomatically, to the closure of the compounds. **(Action: State by December 13, 2016)** [redacted]

- Principals concurred with a number of measures State proposed to take with respect to Russian visas – in particular, leaving to the discretion of State and the Federal Bureau of Investigation (FBI) the issuance of U.S. visas for Russian intelligence officers, holding Russian diplomats to the 48 hour travel notification requirement, and limiting the number of exceptions provided to Russian diplomats. **(Action: State and FBI, ongoing)** [redacted]

- State and FBI will draft, for further legal and policy review, a proposal for removing a number of suspected Russian intelligence officers in the United States. **(Action: State and FBI by December 10, 2016)** [redacted]

- Principals considered the cyber options and recommended against conducting either a spearphishing campaign or a denial of service attack against certain Russian entities. [redacted]

- Principals agreed to recommend sanctioning of certain members of the Russian military intelligence and foreign intelligence chains of command responsible for cyber operations as a response to cyber activity that attempted to influence or interfere with the U.S. elections, if such activity meets the requirements for designation under Executive Order (E.O.) 13694 on *Blocking the Property of certain persons Engaging in Significant Cyber-Enabled Activities*. The Department of the

[redacted]
Classified by: [redacted]
Reason: [redacted]
Declassify on: [redacted]

Treasury will determine if such sanctions are possible under E.O. 13694. **(Action: Treasury by December 16, 2016)** [redacted]

- Principals were divided on whether to issue the designations of Belan and Bogachev under E.O. 13694 as part of the response to Russian interference in our electoral process. Some Principals opposed designations in this context because: (a) the conduct in question was unrelated to the election-related activity; and (b) absent a tie to the elections, any package of designations should include the two Chinese companies for which sanctions packages also have been developed. Other Principals support designations in this context because: (a) a failure by this Administration to use E.O. 13694 will undermine the E.O.'s utility and deterrent effect; and (b) if coupled with appropriate messaging, use of the E.O. against Russian targets would signal that future election-related activity could prompt sanctions. [redacted]

- [redacted]

- [redacted]

- To the maximum extent feasible consistent with sources and methods, Principals agreed to publicly release and attribute to Russian intelligence services technical and other information about: (a) Russian intrusion set; and (b) the recent Russian spearphishing campaign highlighted in intelligence reporting on December 9. The Cyber Response Group (CRG) will coordinate the development of the plan for public release based on input from the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the FBI. **(Action: CRG in coordination with CIA, NSA, and FBI by December 19, 2016)** [redacted]

From: [redacted]-DNI-
Sent: Friday, December 09, 2016 6:24 PM
To: [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]
[redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-
DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-
DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]
[redacted]-DNI-; [redacted]-DNI-; [redacted]; [redacted]-DNI-
Cc: [redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-; [redacted]
[redacted]-DNI-; [redacted]-DNI-; [redacted]-DNI-
Subject: RE: POTUS Tasking on Russia Election Meddling

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

Hello leadership team,

I chatted with [redacted] tonight on our plan.

Our plan is to have CIA/CCI to put together Part B.i and DHS to put together 3 (recommendations to protect). CIA/EEMC is to put together Part B.ii and B.iii.

We will be the NIC firewall for those sections; our team will man the Part B.i and [redacted] team will oversee Part B.ii and B.iii; as we integrate into Part B.iv by **December 23**. We will also generate a draft version for Congressional briefing and an unclassified version.

We will send out for coordination last week of December and first week of January for IC seniors to sign off and aim for delivery by **January 9.**

Our plan is to put this into an ICA with Annexes. We will also decide on how to integrate the DHS recommendation section later.

We will use some part of our summer's ICA on cyber threats to presidential election as a starting point.

[redacted]

(U) [redacted]
======================================
National Intelligence Officer for Cyber Issues
Office of the Director of National Intelligence
[redacted]

From: [redacted]-DNI-
Sent: Friday, December 09, 2016 5:43 PM
To: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted];
[redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-

[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted];
[redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]
[redacted]cia[redacted]; [redacted]-DNI-[redacted]
Subject: POTUS Tasking on Russia Election Meddling

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
=====================================================
```

All,

Pursuant to the POTUS tasking at Monday's meeting on Russia election meddling for a comprehensive assessment, the DNI broached the TPs below with Dennis McDonough and DCIA at the Russia PC this afternoon.

Rather than brief it, he just handed a copy of the TPs to Dennis and mentioned it to DCIA, who both said they were okay with the proposal. I'm sure there may be some bureaucratic hurdles still, but the DNI's directive was to move forward with the paper as outlined. (See below the exact TPs he handed CoS POTUS, which I amended slightly in keeping with the DNI's expressed intent.)

I don't believe they discussed the nitty-gritty as far as format, so we'll have to proceed as we think best.

For reference, I have attached the public statement that ODNI and DHS put out about the Russians before the election, which also included some Q&As that were not published.

Separately, he also promised this assessment to the SSCI in his farewell roundtable. Moreover, we've gotten mail from Congress asking that all members get a classified briefing on the Russia elections issue. My suggestion would be that we draft the classified version of the paper in such a way that we will be able to downgrade it to a (still classified) level that could be shared widely with Congress. (That would be in addition to an unclassified assessment.)

We'll aim to do a thorough backbrief on Monday evening, likely at 1715. I will be in touch on Monday.

[redacted]

TASKER ON RUSSIAN INTERFERENCE IN US ELECTIONS

[redacted] The IC is prepared to produce an assessment per the President's request, that pulls together the information we have on the tools Moscow used and the actions it took to influence the 2016 election, an explanation of why Moscow directed these activities, and how Moscow's approach has changed over time, going back to 2008 and 2012 as reference points. ODNI will lead the effort with participation from CIA, FBI, NSA, and DHS**.**

- The goal would be to produce a highly classified version and an unclassified version:
    - The classified version would include a comprehensive analysis of Russia's activities, drawing from all available sources, with a target delivery date of 9 January to the President.
    - The unclassified version would follow the classified delivery, and to the greatest extent possible would include the same information while still protecting sources and methods. The goal would be to make the unclassified document publicly available.

Details of IC Proposal:

1. Interagency steering group led by ODNI will scope project, ensure access to information, provide coordination and review, and guidance on classification
2. Interagency Tiger Team will draft assessment of "what happened"
    a. CIA, FBI, NSA officers will participate; DHS and OSE analysts will contribute
    b. Assessment will address the following questions
        i. How did Moscow seek to influence the US presidential election in 2016? What tools did they use?
            1. Hacking (CIA, FBI, NSA lead)
            2. Leaks (CIA, FBI, NSA lead)
            3. Cyber activity against voting system (DHS input)
            4. Media spin, trolls, fake news (OSE lead)
            5. Domestic Russian Intelligence efforts (FBI input)
        ii. Why did Moscow direct these activities? What have the Russians hoped to accomplish? (CIA lead)

        iii. How has Moscow’s approach to our elections changed over time? What kinds of activities did they undertake in previous elections? (CIA lead)
        iv. What is our assessment regarding how Moscow will leverage its capabilities in future US elections? (all, NIC lead)

    c. Assessment will include additional elements, such as timeline of key events and Russian actions; a box on China’s role in the 2008 election; Russian election interference in Europe

3. Steering group will provide contributions from DHS for the opportunities/recommendations section of the task.

Questions/issues for the PC to consider:

Will the priority be on developing a paper that can be shared and released or one that is a comprehensive and authoritative account of the Russian activity that took place?

1. **<u>What are the expectations for publicly releasable elements of the assessment?</u>** ODNI proposes that a classified, compartmented assessment to be delivered to POTUS 9 January; broader dissem document and publicly releasable points will be prepared subsequently. Alternatively we could provide a broader dissem Intelligence Community Assessment, with a compartmented annex for PDB customers only.

2. **<u>What are the expectations re: the length and comprehensive nature of the document?</u>** IC proposes a 5-10 page paper with annexes.

[redacted]

Executive Assistant to the DNI

[redacted]

```
=======================================================
Classification: [redacted]

=======================================================
Classification: [redacted]
```

From: [redacted]-DNI-
Sent: Monday, December 12, 2016 12:07 PM
To: [redacted]; [redacted]; [redacted]
Cc: [redacted]-DNI-; [redacted]-DNI-
Subject: FW: Moving forward quickly on Russia/Election tasking

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted]

FYSA - [redacted] officially sent out a note regarding our plan. I wonder if you plan to support us in bringing together the Part i.1-3 below.

[redacted]

[redacted]
==
National Intelligence Officer for Cyber Issues
Office of the Director of National Intelligence
[redacted]

From: [redacted]
Sent: Monday, December 12, 2016 11:28 AM
To: [redacted]-DNI-[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted] NSA-[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted] NSA-[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted] fbi[redacted]; [redacted] fbi[redacted]; [redacted] FBI[redacted]; [redacted]-DNI-[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted] FBI[redacted]; [redacted]-DNI-[redacted]; [redacted] cia[redacted]
Cc: [redacted] cia[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted] cia[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted] cia[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted] cia[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted] cia[redacted]; [redacted] cia[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]
Subject: RE: Moving forward quickly on Russia/Election tasking

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted]

We are meeting with DCIA today at 1230 to discuss a way ahead internally; we'll be back to you after that meeting, at which [redacted], [redacted], and [redacted] will be present.

On the sections you want [redacted] responsible for, I am not sure I agree with this outline; I have also discussed with [redacted] who share my view. I will call to discuss.

From: [redacted]
Sent: Monday, December 12, 2016 11:26 AM
To: [redacted] cia [redacted]; [redacted] cia [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] cia [redacted]; [redacted] -DNI- [redacted]; [redacted]
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] NSA- [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] cia [redacted]; [redacted] cia [redacted]; [redacted]
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] cia [redacted]; [redacted] NSA- [redacted]
[redacted]; [redacted] cia [redacted]; [redacted] cia [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] fbi. [redacted]; [redacted]; [redacted]
[redacted] FBI [redacted]; [redacted] -DNI- [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] cia [redacted]; [redacted] cia [redacted]; [redacted]
[redacted] cia [redacted]; [redacted] FBI [redacted]; [redacted] -DNI-
[redacted]; [redacted] cia [redacted]
Cc: [redacted] cia [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] cia [redacted];
[redacted] -DNI- [redacted]; [redacted] -DNI- [redacted];
[redacted] cia [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI- [redacted];
[redacted] -DNI [redacted]; [redacted] cia [redacted]; [redacted] -DNI-
[redacted]; [redacted] -DNI- [redacted]; [redacted] cia [redacted];
[redacted] cia [redacted]; [redacted] -DNI- [redacted]; [redacted] -DNI-
[redacted]
Subject: Moving forward quickly on Russia/Election tasking
Importance: High

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted]

All: We are moving forward with this tasking. In the wake of Friday's PC and the media frenzy over the weekend, DNI has asked us to move the timeline forward, aiming at a 3 January delivery date. He knows this means many of us will work through the holidays, and expects us to do so. With the expedited timeline in mind, I'd like to have a working draft together by next Wednesday. To do this, we need agencies need to identify the POCs for this right away, and allow them to serve offline for the next week or so. NIO-Cyber [redacted] and I will divide and conquer with you – substantive POCs will hear from either [redacted] or myself for coordinating meetings. We would like CIA's [redacted] to take the lead in drafting for sections 1-3, and CIA's [redacted] to pull together the other sections

i. How did Moscow seek to influence the US presidential election in 2016? What tools did they use?
   1. Hacking ([redacted] lead drafter with CIA, FBI, NSA)
   2. Leaks ([redacted] lead drafter with CIA, FBI, NSA)
   3. Cyber activity against voting system ([redacted] lead drafter with DHS input)
   4. Media spin, trolls, fake news ([redacted] input to [redacted])
   5. Domestic Russian Intelligence efforts (FBI input with NIO-CI/NCSC)

ii. Why did Moscow direct these activities? What have the Russians hoped to accomplish? ([redacted] lead)

iii. How has Moscow's approach to our elections changed over time? What kinds of activities did they undertake in previous elections? ([redacted] lead)

iv. What is our assessment regarding how Moscow will leverage its capabilities in future US elections? (all, NIC lead)

Assessment will include additional elements, such as timeline of key events and Russian actions; a box on China's role in the 2008 election; [redacted] – contributions to be sent in to DNIOs [redacted].

I will keep you updated as we move along.

Best,
[redacted]

[redacted]
National Intelligence Officer for Russia and Eurasia
National Intelligence Council
[redacted]

===
Classification: [redacted]

===
Classification: [redacted]

From: [redacted]-DNI-
Sent: Thursday, December 22, 2016 6:05 PM
To: [redacted]-DNI-; [redacted]-DNI-
Subject: FW: Rollout Planning for IC Report on Russian Election Meddling

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
=====================================================
```

(U) [redacted]
==
National Intelligence Officer for Cyber Issues
Office of the Director of National Intelligence
[redacted]

From: [redacted]-DNI-
Sent: Thursday, December 22, 2016 6:04 PM
To: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]
Subject: RE: Rollout Planning for IC Report on Russian Election Meddling

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
=====================================================
```

Certainly. I'll just emphasize that the Congressional timeline (and gang of 8 briefing) like most of the timeline is just imaginary, based on the presumption that it would be wise to brief Congress sometime between POTUS and the public. No one has directed us to do that, as far as I know.

The only real direction we got was: 1) POTUS wants a comprehensive assessment, drawing from all available sources, and 2) it has to be before the end of his administration.

The initial proposal was 6 and 9 January for the respective classified and unclassified release, which was given to the White House by the DNI. Subsequent to some DNI-DCIA discussion, we moved it up to 3 and 6 January because the feeling was 9 January was already too late in the game. ([redacted], I suspect we did not communicate the new timeline to the WH, hence you heard the originally proposed dates today.)

[redacted]

From: [redacted]-DNI-
Sent: Thursday, December 22, 2016 5:40 PM
To: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]
Subject: RE: Rollout Planning for IC Report on Russian Election Meddling

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
======================================================
```

Thanks [redacted].

In the future, it'd be best of OLA, PAO, and OGC are on the group VTC's or discussions with the DNI addressing rollout planning. We are working with WH and IC Leg and Comms teams, and want to make sure we're all appropriately looped in and discussing the same things.

That said, I was not tracking on a special briefing for Gang of Eight members, and that didn't come up with the WH earlier today. I will follow back up with them to ensure they are aware of that as a potential point on the plan, but will need to discuss with CIA, FBI, and NSA Legislative Affairs before we can confirm that as a step.

This timeline is immensely helpful, thank you. All -- please let us know if you see anything that could potentially slow this trajectory. Per the DNI's earlier request, we are working the engagement list related to this subject from the past months. We will aim to have that complete mid next week.

[redacted]

From: [redacted]-DNI-
Sent: Thursday, December 22, 2016 5:31 PM
To: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-
[redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI[redacted]; [redacted]-DNI-
[redacted]; [redacted]-DNI-[redacted]
Subject: RE: Rollout Planning for IC Report on Russian Election Meddling

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
======================================================
```

Thanks [redacted]. This is a somewhat more aggressive schedule than we had heard earlier today, which had the TS version delivered on or about the 6th, and the unclas version on or about the 9th.

From: [redacted]-DNI-
Sent: Thursday, December 22, 2016 5:30 PM
To: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]
Cc: [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]; [redacted]-DNI-[redacted]
Subject: Rollout Planning for IC Report on Russian Election Meddling

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
=======================================================
```

[redacted],

DNI and folks in the NIC just had a VTC about the IC report on Russian election meddling that POTUS tasked us to do. I wanted to make sure you were up-to-date on the rollout plan as best I can synthesize it, based on multiple incomplete and notional conversations. In other words, this is just a starting point.

Right now we are planning three versions of the report: a high-classified version, a low-classified version, and an unclassified version. The reason for a low-class version is that the high-class version may contain some operationally sensitive details not appropriate for the Congress.

- 3 January – high-class report is delivered to the White House
- 3/4 January (notional) – DCIA, D/FBI, DNI and (DIRNSA, maybe?) brief POTUS on the high-class report
- 3/4 January (notional) – DCIA, D/FBI, DNI and (DIRNSA, maybe?) brief POTUS-elect on the high-class report. (Alternatively: Just DNI + D/FBI or just DNI + DCIA brief P-E.) We are still working out the modalities for the P-E briefing, but the feeling is we should brief P-E first after POTUS.
- 4-6 January (notional) – high-class report is delivered (?) and briefed to the Gang of 8; unclear if we give the paper or just brief it. Maybe all Congress just gets the low-class version.
- 4-6 January (notional) – low-class version of the study is made available to all members of the HPSCI and SSCI.
- 6 January – Unclassified version of the report is released to the public.

[redacted]

[redacted]
Executive Assistant to the DNI
[redacted]

```
=======================================================
Classification: [redacted]
```

```
=======================================================
Classification: [redacted]

=======================================================
Classification: [redacted]

=======================================================
Classification: [redacted]

=======================================================
Classification: [redacted]
```

[redacted]

ICA

INTELLIGENCE COMMUNITY ASSESSMENT

[redacted] Assessing Russian Activities and Intentions in Recent US Elections

ICA 2017-01 | 5 January 2017

CL BY: [redacted] | DRV FRM: [redacted] | DECL ON: [redacted]

[redacted]

[redacted] This report responds to the President's request for a comprehensive assessment of the Russian Government's intentions and actions with respect to recent US elections. The main body of the report was drafted by CIA, FBI, and NSA, and draws on intelligence information collected and disseminated by those three agencies. It covers Moscow's use of cyber tools and media campaigns and its motivation and intention to influence US public opinion.

[redacted] This report is a downgraded version of a more sensitive assessment that has been provided to recipients approved by the President, including House and Senate leadership and the leadership of the intelligence oversight committees. The conclusions in this document are all reflected in the more sensitive assessment, but this document does not include the full supporting information, including specific intelligence on key elements of the influence campaign.

[redacted]

[redacted]

(U) Scope and Sourcing

(U) Information available as of 29 December 2016 was used in the preparation of this product.

(U) Scope

[redacted] This report includes an analytic assessment drafted and coordinated among CIA, FBI, and NSA, which draws on intelligence information collected and disseminated by those three agencies. It covers the motivation and scope of Moscow's intentions regarding US elections and Moscow's use of cyber tools and media campaigns to influence US public opinion. The assessment focuses on activities aimed at the 2016 US presidential election and draws on our understanding of previous Russian influence operations. When we use the term "we," it refers to an assessment by all three agencies.

[redacted] This report does not include an assessment of the impact that the full scope of Russian activities had on the actual outcome of the 2016 election. The US Intelligence Community is charged with monitoring and assessing the intentions, capabilities, and actions of foreign actors; it does not analyze US political processes or US public opinion. We also do not include information from ongoing investigations.

- [redacted] Additional information about Russian cyber activity or supply chain targeting would prompt us to reconsider our assessment about the scope of Russian intelligence and influence efforts during the election.

- (U//[redacted]) For the purposes of this assessment we use DHS's definition of electoral infrastructure that refers to the information, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

(U) Sourcing

[redacted] Many of the key judgments in this assessment rely on a body of reporting from multiple sources that are consistent with our understanding of Russian behavior. Insights into Russian efforts—including specific cyber operations—and Kremlin views of key US players like President-elect Trump and Secretary Clinton derive from multiple corroborating sources.

[redacted] Some of our judgments about Kremlin preferences and intent are drawn from the behavior of Kremlin-loyal political figures, state media, and pro-Kremlin social media actors, all of whom the Kremlin either directly uses to convey messages or who are answerable to the Kremlin. The Russian leadership invests significant resources in both foreign and domestic propaganda and places a premium on transmitting what it views as consistent, self-reinforcing narratives regarding its desires and redlines, whether on Ukraine, Syria, or relations with the United States.

[redacted] Assessing Russian Activities and Intentions in Recent US Elections

ICA 2017-01
5 January 2017

(U) Key Judgments

[redacted] **Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.**

[redacted] **We assess Russian President Vladimir Putin ordered an influence campaign in the summer of 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.** We have high confidence in these judgments based on a body of intelligence reporting and the public behavior of senior Russian officials and state-controlled media. **We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him.** CIA and FBI have high confidence in this judgment based on sensitive information not included in this version of the assessment; NSA has moderate confidence in this judgment based on the same sensitive information. NSA's confidence in this judgment would be elevated to high with additional corroborating sources.

- [redacted] Moscow's approach evolved over the course of the campaign based on Russia's understanding of the electoral prospects of the two main candidates. When Moscow assessed that Secretary Clinton was likely to win the election, the Russian influence campaign began to focus more on undermining her future presidency.

- [redacted] We assess that Moscow refrained from the full spectrum of actions it could have taken to influence the US election. We judge that the Kremlin could have disclosed additional material and could have conducted attacks on electoral infrastructure in the runup to and on Election Day.

- [redacted] Further intelligence has come to light since Election Day that, when combined with Russian behavior since early November 2016, increase our confidence in our assessments of Russian motivations and goals.

[redacted] **Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."** Russia and the Soviet Union have a history of conducting covert influence campaigns focused on US presidential elections, which has used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.

- [redacted] The Russian Foreign Intelligence Service (SVR) and General Staff Main Intelligence Directorate (GRU) both conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties. We have high confidence in this judgment.

- [redacted] We assess with high confidence that the GRU used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusives to media outlets, and that the GRU was directed to pass material it collected to WikiLeaks.

- [redacted] The GRU obtained and maintained access to elements of several confirmed and possibly as many as 20 state or local electoral boards, [redacted] **A DHS assessment indicates the GRU probably was in a position to tamper with some voter registration databases, but that the types of systems Russian actors targeted or compromised were not involved in vote tallying.** It is unclear what the Russian Government intended to accomplish with these intrusions, but they may have been exploratory efforts to determine how vulnerable US electoral systems were to electronic manipulation or preparatory steps to undermine confidence in the election by creating the impression that results had been altered.

- [redacted] Russia's state-run propaganda machine contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences.

[redacted] **We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts.** Moscow would have seen its election influence campaign as at least a qualified success regardless of the outcome of the election because of its perceived ability to impact public discussion in the United States.

- [redacted] **We assess** [redacted] **will be the next major focus of Russian influence operations,** [redacted]

(U) Contents

[redacted] CIA/FBI/NSA Assessment: Russia's Influence Campaign Targeting the 2016 US Presidential Election

(U) Annexes

[redacted]

[redacted] Russia’s Influence Campaign Targeting the 2016 US Presidential Election

(U) Produced jointly under the auspices of the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency.

[redacted]

[redacted] Russia's Influence Campaign Targeting the 2016 US Presidential Election

[redacted] Putin Ordered Campaign To Influence US Election

[redacted] We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign by summer 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. When Moscow assessed later in the year that Secretary Clinton was likely to win the election, its influence campaign then focused on undermining her expected presidency.

- [redacted] We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. CIA and FBI have high confidence in this judgment based on sensitive information not included in this version of the assessment; NSA has moderate confidence in this judgment based on the same sensitive information. NSA's confidence would be elevated to high with additional corroborating sources.
- [redacted] In trying to influence the US election, we assess the Kremlin sought to advance its longstanding desire to undermine the US-led liberal democratic order, the promotion of which Putin and other senior Russian leaders view as a threat to Russia and Putin's regime. [redacted]

[redacted]

- [redacted] Putin believed the Panama Papers disclosure and the Olympic doping scandal were US-directed efforts to defame Russia, judging from [redacted] and his public comments, suggesting he sought to use disclosures to discredit the image of the United States and cast it as hypocritical.

[redacted] Putin most likely wanted his intelligence services to discredit Secretary Clinton because he has blamed her since 2011 for inciting mass protests against his regime in late 2011 and early 2012 and holds a grudge for comments he almost certainly saw as disparaging him, judging from press reporting. Given this, we assess with high confidence that the GRU was directed to pass material it collected to WikiLeaks and other intermediaries.

[redacted] We assess Putin, his advisers, and the Russian Government developed a clear preference for President-elect Trump over Secretary Clinton. We base this assessment on [redacted] and Russian state media indicating that Russian officials saw President-elect Trump as more favorable to key Russian interests and more in line with Putin's preference for leaders he views as dealmakers. Throughout the election, Russian Government officials characterized Secretary Clinton and Democratic politicians as particularly unfriendly to Russian interests, [redacted]

- [redacted]

[redacted]

- [redacted] Beginning in June, Putin's public comments about the US presidential race avoided directly praising President-elect Trump, probably because Kremlin officials thought that any praise from Putin personally would backfire in the United States. Nonetheless, Putin publicly indicated a preference for the President-elect's stated policy to work with Russia, and pro-Kremlin figures spoke highly about what they saw as his Russia-friendly positions on Syria and Ukraine. Putin contrasted President-elect Trump's approach to Russia with Secretary Clinton's "aggressive rhetoric," according to Russian press reporting.

- [redacted] Moscow also saw the election of President-elect Trump as a way to achieve an international counterterrorism coalition against the Islamic State in Iraq and the Levant (ISIL), according to diplomatic reporting. The Kremlin has historically preferred Republican over Democratic candidates, judging that Republicans had been less focused on democracy and human rights and were therefore easier to deal with, [redacted]

- [redacted] Putin has had many positive experiences working with Western political leaders whose business interests, Moscow assessed, made them more disposed to deal with Russia, such as former Italian Prime Minister Silvio Berlusconi and former German Chancellor Gerhard Schroeder, judging from [redacted] and press reporting [redacted]

- [redacted] Putin, Russian officials, and other pro-Kremlin pundits stopped publicly criticizing the US election process as unfair almost immediately after the election because Moscow probably assessed it would be counterproductive to building positive relations.

[redacted] We assess the influence campaign aspired to help President-elect Trump's chances of victory when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to the President-elect. Later in the summer, senior Russian diplomats and intelligence officers assessed Secretary Clinton was likely to win the presidency, judging from [redacted] and Russian press reporting. As a result, we assess the Russian Government began to focus more on undercutting Secretary Clinton's legitimacy and crippling her presidency from its start, including by impugning the fairness of the election. Moscow therefore held back some pre-election influence efforts for potential later use.

- [redacted] Before the election, Russian diplomats had both publicly denounced the US electoral process and privately developed plans to publicly call into question the validity of the results, [redacted] Pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, according to well-informed Russian journalists.

- [redacted] Moscow had additional information it obtained from cyber collection against US government and non-government targets that it could have used against a Clinton Administration's policies and nominees, based on [redacted] Russian intelligence collection efforts.

[redacted] Russian Campaign Was Multifaceted

[redacted]) Moscow's use of disclosures during the US election was unprecedented, but its influence campaign otherwise followed a longstanding Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."

- [redacted] Putin approves influence campaigns—particularly those that would be politically sensitive—gives strategic guidance, and delegates tactical moves to Russian agencies and their officers to pursue independently, [redacted]

- [redacted] Moscow's campaign aimed at the US election reflected years of investment in its capabilities, which Moscow has honed in the former Soviet states, [redacted]

- [redacted] By their nature, Russian influence campaigns are multifaceted and difficult to attribute to a given decisionmaking center or individual because they use a mix of agents of influence, cutouts, front organizations, and false-flag operations designed to create deniability. Moscow demonstrated this during the Ukraine crisis in 2014, when Putin, we judged, had authorized Russia's involvement in eastern Ukraine, denied it publicly, and delegated aspects of implementation to Kremlin advisers, military officers, and separatist leaders.

[redacted] The Kremlin's campaign aimed at the US election featured disclosures of data obtained through Russian cyber operations via WikiLeaks, as well as via the Guccifer 2.0 persona[a] and DCLeaks.com, which are both likely GRU operations; GRU intrusions into US state electoral infrastructure; and overt propaganda. Russian foreign intelligence collection both informed and enabled the influence campaign, [redacted]

[redacted] ***Cyber Espionage Against US Political Organizations.*** We assess that the SVR and GRU both conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties. We have high confidence in this assessment because it is based on a body of [redacted] intelligence reporting that reinforces and elaborates on publicly available commercial cyber analyses.

- [redacted]) Despite the Russian intelligence services' generally sophisticated cyber operations, their large-scale approach and human error in execution created opportunities to gain insight into their efforts through intelligence collection.

([redacted]) We assess the SVR conducted foreign intelligence collection against the US primary campaigns and on think tanks and lobbying groups likely to shape future US policies. In July 2015, the SVR gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016, [redacted] Separate [redacted] intelligence indicates that the SVR by late 2015 had gained and maintained access to think tanks and political groups from which they collected intelligence on the election campaign.

- [redacted] SVR collected material was provided as foreign intelligence reports to senior Russian officials, [redacted]

[redacted] The GRU probably began cyber operations aimed at the US election by March 2016, [redacted] The GRU was preparing a spearphishing operation to target Secretary Clinton's staff and the Democratic Party, other political targets, foreign governments, and NGO employees.

- [redacted] We assess that the campaign, which ran from March through July 2016, resulted in the compromise of the personal

[a] (U) The persona referring to itself as "Guccifer 2.0" claims it chose its name in homage to Guccifer, an imprisoned Romanian hacker named Marcel Lazar, who hacked and publicly disclosed information from the email accounts of an adviser to Secretary Clinton and others. The communications revealed the existence of Secretary Clinton's personal email server. Guccifer also claimed to have hacked Secretary Clinton's personal email server, but later admitted he invented the claim.

e-mail accounts of Democratic Party officials and political figures, [redacted]. By May, GRU cyber infrastructure had connected to the DNC and exfiltrated large volumes of data, [redacted]

- [redacted] GRU actors in early July used known GRU infrastructure to log in to e-mail accounts belonging to state- and federal-level Republican campaigns and several Political Action Committees (PACs) supporting that party, according to CIA analysis of [redacted] technical data. We assess with high confidence that the GRU targeted a company that managed domains for Republican campaigns and PACs and a domain that the Republican National Committee (RNC) had previously used. GRU efforts compromised entire e-mail accounts, [redacted] RNC officials told the FBI that the domain had not been used for at least six years.

- [redacted]

[redacted] ***Public Disclosures of Russian-Collected Data.*** We assess the GRU used both the Guccifer 2.0 persona and DCLeaks.com operationally to release US data obtained in GRU cyber operations publicly and in exclusives to media outlets. We have high confidence that Guccifer 2.0 and DCLeaks.com published GRU-hacked data, but moderate confidence that they were under direct GRU control [redacted]. We base our judgments on several factors: the information that was disclosed was information we assess the GRU accessed as part of its operations against US political targets; the initial data leak occurred the day after the US cybersecurity firm CrowdStrike publicized Russia's intrusion into the DNC; and signals intelligence placed the operators of Guccifer 2.0 and DCLeaks.com in Russia.

- [redacted] Guccifer 2.0, who claimed to be an independent Romanian hacker, made multiple contradictory statements and false claims about his identity throughout the election; [redacted] intelligence indicated the persona was controlled from Russia, and press reporting suggests more than one person claiming to be Guccifer 2.0 interacted with journalists, based on [redacted] and interactions with the press.

- [redacted]) Content that we assess was taken from [redacted] e-mail accounts targeted in March 2016 by a GRU cyber espionage unit subsequently appeared on DCLeaks.com in June.

- [redacted] On several occasions, the administrators of Guccifer 2.0 and DCLeaks.com logged in to accounts associated with those personas using a Russia-based mobile broadband provider [redacted] although they generally attempted to obscure the source of their Internet traffic.

[redacted] We assess that the GRU was directed to pass material it acquired from the DNC to WikiLeaks. We have high confidence in this judgment. We assess that the Russian Government also passed to WikiLeaks material collected on a senior Democratic Party official. We lack insight into whether WikiLeaks was witting of Russian involvement in either case and whether the Russian Government controlled the timing and content of releases. [redacted]

- [redacted] In early September, Putin deflected a reporter's question about Russian Government involvement in the disclosure of DNC data to WikiLeaks, saying publicly it was important the data was exposed, calling the search for the source of the leaks a distraction, and denying Russian "state-level" involvement.

- [redacted]) Moscow most likely chose WikiLeaks because of its self-proclaimed reputation for authenticity. Disclosures through WikiLeaks did not contain any evident forgeries. As part of its disclosures related to a senior Democratic Party official, WikiLeaks released the original spearphishing e-mail that we assess GRU cyber actors created.
- [redacted] The Kremlin's principal international propaganda outlet RT (formerly Russia Today) has actively collaborated with WikiLeaks. RT's editor-in-chief visited WikiLeaks founder Julian Assange at the Ecuadorian Embassy in London in August 2013, where they discussed renewing his broadcast contract with RT, according to Russian and Western media. Russian media subsequently announced that RT had become "the only Russian media company" to partner with WikiLeaks and had received access to "new leaks of secret information." RT routinely gives Assange sympathetic coverage and provides him a platform to denounce the United States.

[redacted] These election-related disclosures reflect a pattern since 2014 of the GRU using hacked information in targeted influence efforts against targets such as Olympic athletes and other foreign governments. Such efforts have included releasing or altering personal data, defacing websites, or releasing e-mails.

- [redacted] A prominent target since the 2016 Summer Olympics has been the World Anti-Doping Agency, with leaks that we assess to have originated with the GRU and that have involved data on US athletes.

[redacted] Although we saw Russian collection on some Republican-affiliated targets, [redacted]

[redacted] ***Russian Cyber Intrusions Into State Electoral Infrastructure.*** The GRU accessed elements of several confirmed and possibly as many as 20 state or local electoral boards, [redacted] and it was probably in a position to tamper with at least some voter registration databases, according to a DHS assessment. It is unclear what the Russian Government intended to accomplish with these intrusions, but they may have been exploratory efforts to determine how vulnerable US electoral systems were to electronic manipulation or preparatory steps to undermine confidence in the election by creating the impression that results had been altered.

- [redacted] In late June and early July 2016, probable GRU cyber actors compromised a California voter registration organization's e-mail account, [redacted]
- [redacted] Unidentified actors using GRU infrastructure on 12 July compromised the Illinois State Voter Information Center using seven Internet Protocol (IP) addresses registered to King Servers, a Russian company that provides virtual private network (VPN) services that obscure the source of Internet traffic, [redacted]
- [redacted] Since early 2014, US-based Russian intelligence officers have collected on US electoral processes and related technology and equipment, [redacted]; such collection probably fed GRU targeting efforts.

[redacted] Unidentified actors operating from leased commercial infrastructure commonly used in GRU operations also targeted US state and local voter registration systems. We have low confidence in attributing these reports to the GRU because such services are commonly used by cybercriminals, who probably conducted at least some of the intrusion attempts to collect personally identifiable information on US victims.

- [redacted] State governments, using DHS-provided sensors, detected Internet traffic between the King Servers IP addresses and 18 states from June to early November 2016, and 13 of those states reported malicious activity related to one of the reported IP addresses.

- [redacted] As of January 2016, an e-mail address associated with a suspected GRU actor made connections to the King Servers domain. The suspected GRU actor had leased VPN services from King Servers through December 2009, a gap of several years, [redacted]

[redacted] The types of systems we observed Russian actors targeting or compromising are not involved in vote tallying. We have not detected the sorts of Russian Government cyber accesses that would have allowed Moscow to alter vote tabulations. Additional intelligence information on Russian cyber activity or supply chain targeting of election-related hardware or software would prompt us to reconsider our assessment about the scope of Russian intelligence efforts during the election.

- [redacted]) Between December 2015 and June 2016, GRU cyber actors scanned an identified US-based third-party vendor of electronic voting equipment and services, [redacted].

[redacted] ***Russian Propaganda Efforts.*** Russia's state-run propaganda machine—comprised of its domestic media apparatus, outlets targeting global audiences such as RT and Sputnik, and a network of quasi-government trolls—contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences. State-owned Russian media made increasingly favorable comments about President-elect Trump as the 2016 US general and primary election campaigns progressed while consistently offering negative coverage of Secretary Clinton.

- [redacted] Russian state-owned media coverage of President-elect Trump early in the primaries characterized him as just one of several "fringe" figures who had a minimal chance to win but high potential to disrupt the US political system. English-language RT Online featured an editorial on 7 February 2016 on the Republican primaries in which it called President-elect Trump part of the "Republican radical fringe," and a pro-Kremlin expert wrote the same week that his victory would be a "fundamental disruption" of the US political system.

- [redacted] Starting in March 2016, Russian Government–linked actors began openly supporting President-elect Trump's candidacy in media aimed at English-speaking audiences. RT and Sputnik—another government-funded outlet producing pro-Kremlin radio and online content in a variety of languages for international audiences—consistently cast President-elect Trump as the target of unfair coverage from traditional US media outlets that they claimed were subservient to a corrupt political establishment.

- [redacted] Russian media hailed President-elect Trump's victory as a vindication of Putin's advocacy of global populist movements—the theme of Putin's annual conference for Western academics in October 2016—and the latest example of Western liberalism's collapse, according to [redacted] Russian and Western press reporting.

[redacted] As the US presidential campaign progressed, Kremlin support for President-elect Trump was evident in domestic media coverage, coincident with the broader influence campaign. Putin's chief propagandist Dmitriy Kiselev used his flagship weekly newsmagazine program this fall to cast President-elect Trump as an outsider victimized by a corrupt political establishment and faulty democratic election process that aimed to prevent his election because of his desire to work with Moscow, judging from Russian state media and [redacted] international press reporting.

- [redacted] Pro-Kremlin proxy Vladimir Zhirinovskiy, leader of the nationalist Liberal Democratic Party of Russia, proclaimed just before the election that if President-elect Trump won, Russia would "drink Champagne" in anticipation of being able to advance its positions on Syria and Ukraine. The head of Russia's most prestigious public polling center told a Washington audience later in November that Russians regarded the election results as another in what they see as a series of Putin's successes.

- [redacted] Kremlin-controlled media sometimes communicated support for the President-elect by attacking Secretary Clinton for her positions on the Middle East and then citing President-elect Trump's position on the same issues.

[redacted] RT's coverage of Secretary Clinton throughout the US presidential campaign was consistently negative and focused on her leaked e-mails; alleged corruption, poor physical and mental health, and ties to Islamic extremism. Some Russian officials echoed Russian influence campaign talking points that Secretary Clinton's election could lead to a war between the United States and Russia.

- [redacted]) In August, a think tank the Kremlin uses to privately channel pro-regime messaging to Russian domestic and international media suggested avenging Western reports on Putin's health by airing segments devoted to Secretary Clinton's alleged health problems, [redacted]

- ([redacted]) On 6 August, RT published an English-language video called "Julian Assange Special: Do WikiLeaks Have the E-mail That'll Put Clinton in Prison?" and an exclusive interview with Assange entitled "Clinton and ISIS Funded by the Same Money." RT's most popular video on Secretary Clinton, "How 100% of the Clintons' 'Charity' Went to...Themselves," had more than 9 million views on social media platforms. RT's most popular English language video about the President-elect, called "Trump Will Not Be Permitted To Win," featured Assange and had 2.2 million views.

- ([redacted]) For more on Russia's past media efforts, please see Annex A: Russia—Kremlin's TV Seeks To Influence Politics, Fuel Discontent in US.

([redacted]) Other Russian Influence Efforts

([redacted]) Some Russian influence efforts appeared to be short lived or have little traction, [redacted]

- ([redacted]) [redacted] indicates Russian officials were unable to conduct their desired election monitoring plan because US officials denied their access.

- ([redacted]) [redacted] indicates plans for a Russian-language newspaper supportive of President-elect Trump to be published in the United States were scaled back in late October after Moscow deemed the President-elect's chances for victory to be unlikely.

[redacted]

([redacted]) [redacted] using trolls as well as RT as part of its influence efforts to denigrate Secretary Clinton. [redacted] amplified stories on scandals about Secretary Clinton and the role of WikiLeaks in the election campaign, including an article claiming that she allegedly considered killing Assange.

- [redacted] [redacted] indicates the likely financier of the so-called Internet Research Agency of professional trolls located in Saint Petersburg, close Putin ally Yevgeniy Prigozhin, has confirmed ties to the GRU. We are working to determine the further extent of ties between the Internet Research Agency and the Russian intelligence services.

- [redacted] A journalist who is a leading expert on the Internet Research Agency claimed that some social media accounts that appear to be tied to Russia's professional trolls—because they previously were devoted to supporting Russian actions in Ukraine—started to advocate for the President-elect as early as December 2015.

[redacted] Influence Effort Was Boldest Yet in the US

[redacted] Russia's effort to influence the 2016 US presidential election represented a significant escalation in directness, level of activity, and scope of effort compared to previous operations aimed at US elections. We assess the 2016 influence campaign reflected the Kremlin's recognition of the worldwide effects that mass disclosures of US Government and other private data—such as those conducted by WikiLeaks and others—have achieved in recent years, and their understanding of the value of orchestrating such disclosures to maximize the impact of compromising information. [redacted] reporting and [redacted] indicate that since the collapse of the Soviet Union Moscow had crafted plans to influence previous US presidential elections, but we cannot confirm they were executed.

- [redacted] In 2011, US-based Russian officials had a draft plan to influence the 2012 US presidential election, [redacted] The plan advocated exploiting the *Citizens United* Supreme Court ruling to fund candidates supporting Russian interests, eventually creating a pro-Russia PAC to openly advance Moscow's agenda. SVR officers in San Francisco were tasked to compile information on US firms with ties to Russia, [redacted], possibly in support of this plan; we have no information to indicate the plan was implemented.

- [redacted] In 1999, the SVR's San Francisco base developed a plan to use a contact to promulgate Russian views in US political parties' campaign platforms and among candidates for the presidential election in 2000, [redacted]

- (U) During the Cold War, the Soviet Union used intelligence officers, influence agents, forgeries, and press placements to disparage candidates perceived as hostile to the Kremlin, according to former KGB archivist Vasiliy Mitrokhin.

[redacted] Past Russian intelligence efforts related to US elections have primarily focused on foreign intelligence collection. For decades, Russian and Soviet intelligence services have sought to collect insider information from US political parties that could help Russian leaders understand a new US administration's plans and priorities.

- [redacted]In 2008, all Russian consular offices were required to report any information about the likely outcome of the US presidential election, potential cabinet members of the new administration, the impact of the US economy on the election, and the new administration's policies toward Russia, [redacted] The SVR Directorate S (Illegals) officers arrested in the United States in 2010 also reported to Moscow about the 2008 election.

- (U) In the 1970s, the KGB recruited a Democratic Party activist who reported information about then-presidential hopeful Jimmy Carter's campaign and foreign policy plans, according to Mitrokhin.

[redacted]) 2016 Influence Campaign Could Have Been More Extensive

[redacted] We assess that Moscow refrained from the full spectrum of actions it could have taken to affect the US election. We judge that the Kremlin could have disclosed additional material and could have conducted attacks on electoral infrastructure in the runup to and on Election Day.

- [redacted] The GRU may have compromised additional personal e-mail accounts of leading US political figures from both parties, judging from [redacted] reporting on the extent of its spearphishing campaign from March through June. The contents of any additional compromised email accounts have yet to be disclosed.

- [redacted] We did not detect extensive [redacted] influence operations as part of the Kremlin's campaign. The [redacted] may not have released additional materials, fearing loss of accesses that would have endangered continued collection on US decisionmaking in a Clinton administration, [redacted]

- [redacted] We did not see any forgeries disclosed during the Russian influence campaign. Russian intelligence services have used fabricated information for active measures in numerous past campaigns, according to [redacted] press reporting, and probably could have done so on this occasion.

- [redacted] We assess the GRU refrained from conducting attacks against the electoral infrastructure to which it had access. It is unclear why the GRU did not conduct attacks; it may have refrained from doing so because it lacked the technical capabilities, did not have what it judged to be sufficient access to create desired disruptive effects, or lacked approval for disruption operations.

[redacted] Election Operation Signals "New Normal" in Russian Influence Efforts

[redacted] We assess Moscow will apply lessons learned from its campaign aimed at the US presidential election to future influence efforts in the United States and worldwide. We assess the Russian intelligence services would have seen their election influence campaign as at least a qualified success regardless of the outcome of the election because of their perceived ability to impact public discussion in the United States.

- [redacted] Putin's [redacted] views of the disclosures suggest the Kremlin and the intelligence services will continue to consider using cyber-enabled disclosure operations because of their belief that these can accomplish Russian goals relatively easily without significant damage to Russian interests. We have not yet seen signs that US actions announced in late December 2016 have changed this belief.

- [redacted] Putin's satisfaction at the public attention paid to the influence effort, [redacted] underlines the value he assigns to these sorts of efforts.

[redacted] We assess Germany's federal elections in September 2017 will be the next major focus of Russian influence operations. [redacted]

- [redacted]) Russian intelligence has conducted cyber espionage operations against German think tanks and politicians, giving Russia material it could leak in a similar manner to the US influence campaign, judging from a body of intelligence reporting. [redacted]

[redacted]

- [redacted]) Russia has influenced or sought to influence election campaigns in France, Montenegro, and Moldova, [redacted]
- [redacted]) For more on Russian activities in Europe, please see Annex B: Moscow's Efforts to Manipulate Foreign Elections, 2000-16.

[redacted]) We assess Russian intelligence services will continue to develop capabilities to provide Putin with options to use against the United States, judging from past practice and current efforts. Immediately after Election Day, the SVR probably began a spearphishing campaign targeting US Government employees and individuals associated with US think tanks and NGOs in national security, defense, and foreign policy fields, [redacted] This campaign could provide material for future influence efforts as well as foreign intelligence collection on the incoming administration's goals and plans.

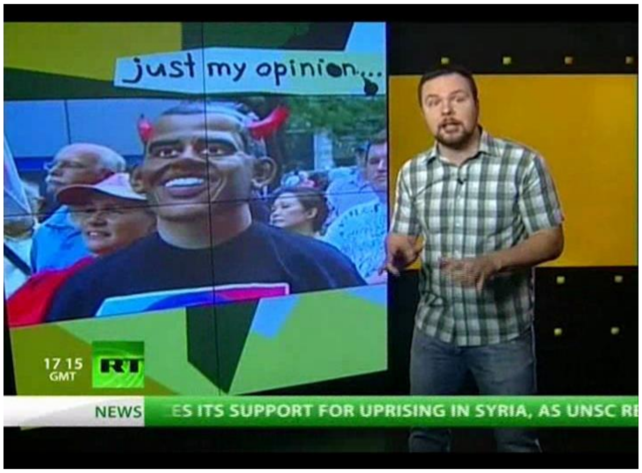
- [redacted]) Russia's demonstrated ability to gain access to at least some US electoral infrastructure, [redacted] suggests that enhanced efforts by the services could threaten the integrity of future votes.
- [redacted] The Kremlin's financial and material support to actors advancing its interests within the United States can be covertly supplied online, through cutouts, or during meetings in Russia or other countries. [redacted]

(U) Annex A

(U) *Russia* -- Kremlin's TV Seeks To Influence Politics, Fuel Discontent in US, 11 December 2012

(U) RT America TV, a Kremlin-financed channel operated from within the United States, has substantially expanded its repertoire of programming that highlights criticism of alleged US shortcomings in democracy and civil liberties. The rapid expansion of RT's operations and budget and recent candid statements by RT's leadership point to the channel's importance to the Kremlin as a messaging tool and indicate a Kremlin-directed campaign to undermine faith in the US Government and fuel political protest. The Kremlin has committed significant resources to expanding the channel's reach, particularly its social media footprint. A reliable UK report states that RT recently was the most-watched foreign news channel in the UK. RT America has positioned itself as a domestic US channel and has deliberately sought to obscure any legal ties to the Russian Government.

(U) In the runup to the 2012 US presidential election in November, English-language channel RT America -- created and financed by the Russian Government and part of Russian Government-sponsored RT TV (see textbox 1) -- intensified its usually critical coverage of the United States. The channel portrayed the US electoral process as undemocratic and featured calls by US protesters for the public to rise up and "take this government back."

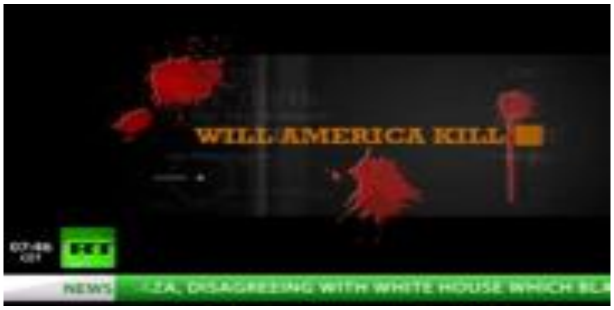


(U) *Messaging on RT prior to the US presidential election (RT, 3 November)*

- (U) RT introduced two new shows -- "Breaking the Set" on 4 September and "Truthseeker" on 2 November -- both overwhelmingly focused on criticism of US and Western governments as well as the promotion of radical discontent.

- (U) From August to November 2012, RT ran numerous reports on alleged US election fraud and voting machine vulnerabilities, contending that US election results cannot be trusted and do not reflect the popular will.
- (U) In an effort to highlight the alleged "lack of democracy" in the United States, RT broadcast, hosted, and advertised third-party candidate debates and ran reporting supportive of the political agenda of these candidates. The RT hosts asserted that the US two-party system does not represent the views of at least one-third of the population and is a "sham."

- (U) RT aired a documentary about the Occupy Wall Street movement on 1, 2, and 4 November. RT framed the movement as a fight against "the ruling class" and described the current US political system as corrupt and dominated by corporations. RT advertising for the documentary featured Occupy movement calls to "take back" the government. The documentary claimed that the US system cannot be changed democratically, but only through "revolution." After the 6 November US presidential election, RT aired a documentary called "Cultures of Protest," about active and often violent political resistance (RT, 1-10 November).



(U) *RT new show "Truthseeker" (RT, 11 November)*

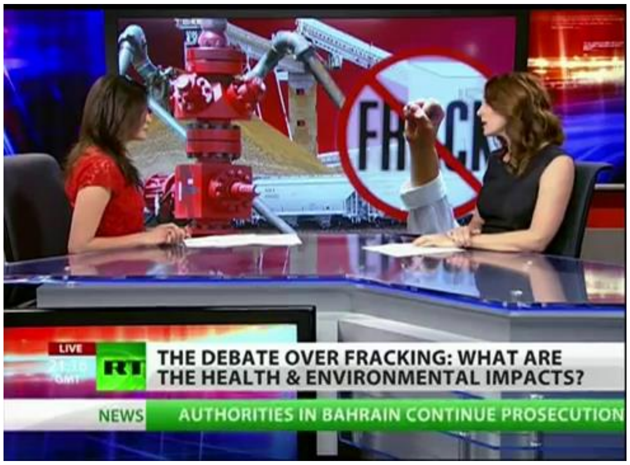
(U) RT Conducts Strategic Messaging for Russian Government

(U) RT's criticism of the US election was the latest facet of its broader and longer-standing anti-US messaging likely aimed at undermining viewers' trust in US democratic procedures and undercutting US criticism of Russia's political system. RT Editor in Chief Margarita Simonyan recently declared that the United States itself lacks democracy and that it has "no moral right to teach the rest of the world" (*Kommersant*, 6 November).

- (U) Simonyan has characterized RT's coverage of the Occupy Wall Street movement as "information warfare" that is aimed at promoting popular dissatisfaction with the US Government. RT created a *Facebook* app to connect Occupy Wall Street protesters via social media. In addition, RT featured its own hosts in Occupy rallies ("Minaev Live," 10 April; RT, 2, 12 June).
- (U) RT's reports often characterize the United States as a "surveillance state" and allege widespread infringements of civil liberties, police brutality, and drone use (RT, 24, 28 October, 1-10 November).
- (U) RT has also focused on criticism of the US economic system, US currency policy, alleged Wall Street greed, and the US national debt. Some of RT's hosts have compared the United States to Imperial Rome and have predicted that government corruption and "corporate greed" will lead to US financial collapse (RT, 31 October, 4 November).

(U) Simonyan steps over the White House in the introduction from her short-lived domestic show on REN TV (REN TV, 26 December 2011)

(U) RT broadcasts support for other Russian interests in areas such as foreign and energy policy.


LIVE
RT
THE DEBATE OVER FRACKING: WHAT ARE THE HEALTH & ENVIRONMENTAL IMPACTS?
NEWS
AUTHORITIES IN BAHRAIN CONTINUE PROSECUTION

(U) RT anti-fracking reporting (RT, 5 October)

- (U) RT runs anti-fracking programming, highlighting environmental issues and the impacts on public health. This is likely reflective of the Russian Government's concern about the impact of fracking and US natural gas production on the global energy market and the potential challenges to Gazprom's profitability (5 October).
- (U) RT is a leading media voice opposing Western intervention in the Syrian conflict and blaming the West for waging "information wars" against the Syrian Government (RT, 10 October-9 November).
- (U) In an earlier example of RT's messaging in support of the Russian Government, during the Georgia-Russia military conflict the channel accused Georgians of killing civilians and organizing a genocide of the Ossetian people. According to Simonyan, when "the Ministry of Defense was at war with Georgia," RT was "waging an information war against the entire Western world" (*Kommersant*, 11 July).

(U) In recent interviews, RT's leadership has candidly acknowledged its mission to expand its US audience and to expose it to Kremlin messaging. However, the leadership rejected claims that RT interferes in US domestic affairs.

- (U) Simonyan claimed in popular arts magazine *Afisha* on 3 October: "It is important to have a channel that people get used to, and then, when needed, you show them what you need to show. In some sense, not having our own foreign broadcasting is the same as not having a ministry of defense. When there is no war, it looks like we don't need it. However, when there is a war, it is critical."
- (U) According to Simonyan, "the word 'propaganda' has a very negative connotation, but indeed, there is not a single international foreign TV channel that is doing something other than promotion of the values of the country that it is broadcasting from." She added that "when Russia is at war, we are, of course, on Russia's side" (*Afisha*, 3 October; *Kommersant*, 4 July).
- (U) TV-Novosti director Nikolov said on 4 October to the Association of Cable Television that RT builds on worldwide demand for "an alternative view of the entire world." Simonyan asserted on 3 October in *Afisha* that RT's goal is "to make an alternative channel that shares information unavailable elsewhere" in order to "conquer the audience" and expose it to Russian state messaging (*Afisha*, 3 October; *Kommersant*, 4 July).
- (U) On 26 May, Simonyan tweeted with irony: "Ambassador McFaul hints that our channel is interference with US domestic affairs. And we, sinful souls, were thinking that it is freedom of speech."

(U) RT Leadership Closely Tied to, Controlled by Kremlin

(U) RT Editor in Chief Margarita Simonyan has close ties to top Russian Government officials, especially Presidential Administration Deputy Chief of Staff Aleksey Gromov, who reportedly manages political TV coverage in Russia and is one of the founders of RT.

- (U) Simonyan has claimed that Gromov shielded her from other officials and their requests to air certain reports. Russian media consider Simonyan to be Gromov's protege (*Kommersant*, 4 July; Dozhd TV, 11 July).
- (U) Simonyan replaced Gromov on state-owned Channel One's Board of Directors. Government officials, including Gromov and Putin's Press Secretary Peskov were involved in creating RT and appointing Simonyan (*Afisha*, 3 October).
- (U) According to Simonyan, Gromov oversees political coverage on TV, and he has periodic meetings with media managers where he shares classified information and discusses their coverage plans. Some opposition journalists, including Andrey Loshak, claim that he also ordered media attacks on opposition figures (*Kommersant*, 11 July).

(U) *Simonyan shows RT facilities to then Prime Minister Putin. Simonyan was on Putin's 2012 presidential election campaign staff in Moscow (*Rospress*, 22 September 2010,* Ria Novosti*, 25 October 2012).*

(U) The Kremlin staffs RT and closely supervises RT's coverage, recruiting people who can convey Russian strategic messaging because of their ideological beliefs.

- (U) The head of RT's Arabic-language service, Aydar Aganin, was rotated from the diplomatic service to manage RT's Arabic-language expansion, suggesting a close relationship between RT and Russia's foreign policy apparatus. RT's London Bureau is managed by Darya Pushkova, the daughter of Aleksey Pushkov, the current chair of the Duma Russian Foreign Affairs Committee and a former Gorbachev speechwriter (*DXB*, 26 March 2009; *MK.ru*, 13 March 2006).
- (U) According to Simonyan, the Russian Government sets rating and viewership requirements for RT and, "since RT receives budget from the state, it must complete tasks given by the state." According to Nikolov, RT news stories are written and edited "to become news" exclusively in RT's Moscow office (Dozhd TV, 11 July; *AKT*, 4 October).
- (U) In her interview with pro-Kremlin journalist Sergey Minaev, Simonyan complimented RT staff in the United States for passionately defending Russian positions on the air and in social media.

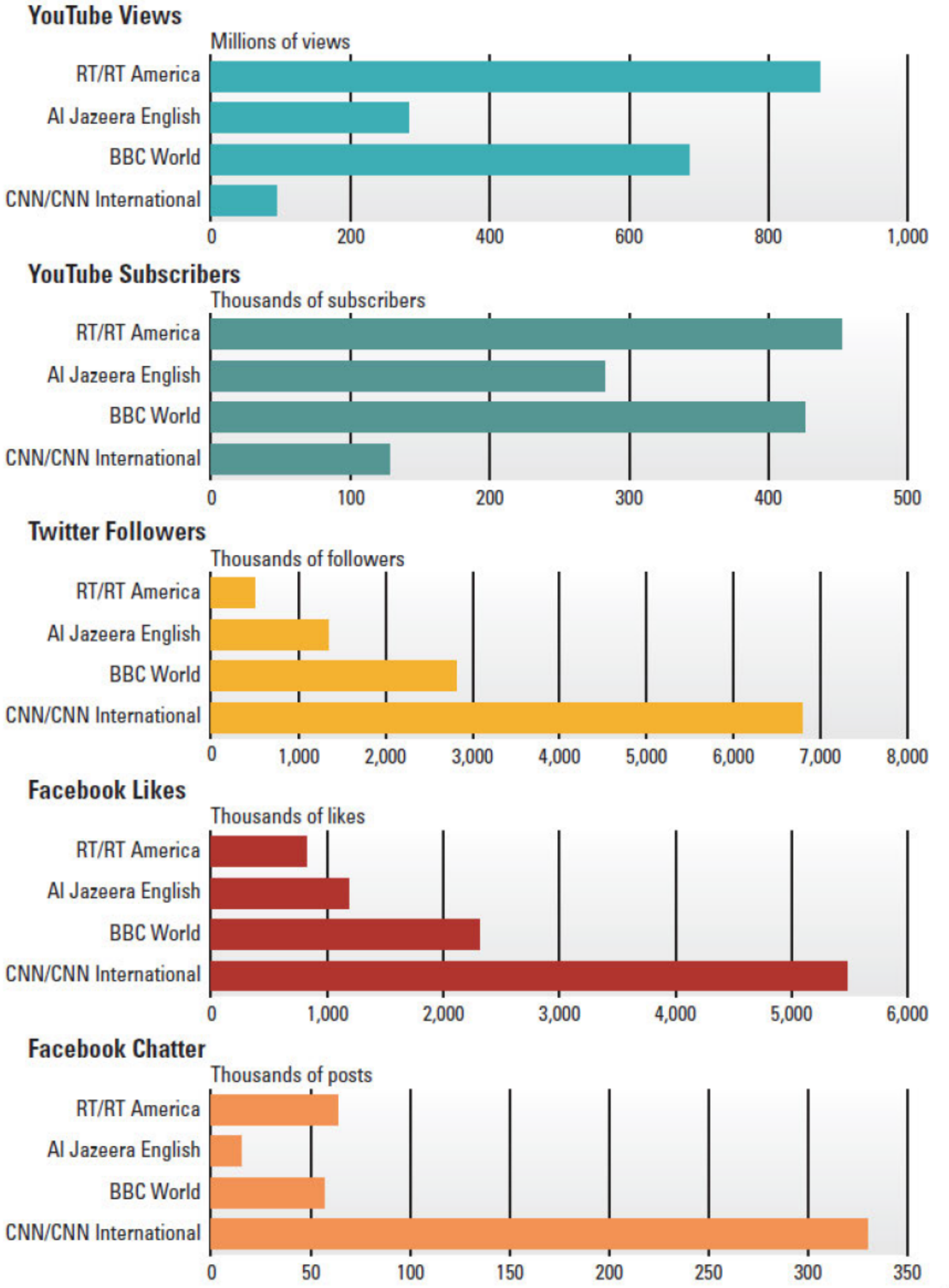
Simonyan said: "I wish you could see…how these guys, not just on air, but on their own social networks, *Twitter*, and when giving interviews, how they defend the positions that we stand on!" ("Minaev Live," 10 April).

(U) RT Focuses on Social Media, Building Audience

(U) RT aggressively advertises its social media accounts and has a significant and fast-growing social media footprint. In line with its efforts to present itself as anti-mainstream and to provide viewers alternative news content, RT is making its social media operations a top priority, both to avoid broadcast TV regulations and to expand its overall audience.

- (U) According to RT management, RT's website receives at least 500,000 unique viewers every day. Since its inception in 2005, RT videos received more than 800 million views on *YouTube* (1 million views per day), which is the highest among news outlets (see graphics for comparison with other news channels) (*AKT*, 4 October).
- (U) According to Simonyan, the TV audience worldwide is losing trust in traditional TV broadcasts and stations, while the popularity of "alternative channels" like RT or Al Jazeera grows. RT markets itself as an "alternative channel" that is available via the Internet everywhere in the world, and it encourages interaction and social networking (*Kommersant*, 29 September).
- (U) According to Simonyan, RT uses social media to expand the reach of its political reporting and uses well-trained people to monitor public opinion in social media commentaries (*Kommersant*, 29 September).
- (U) According to Nikolov, RT requires its hosts to have social media accounts, in part because social media allows the distribution of content that would not be allowed on television (*Newreporter.org*, 11 October).
- (U) Simonyan claimed in her 3 October interview to independent TV channel Dozhd that Occupy Wall Street coverage gave RT a significant audience boost.

TV News Broadcasters: Comparative Social Media Footprint



[redacted]

(U) The Kremlin spends $190 million a year on the distribution and dissemination of RT programming, focusing on hotels and satellite, terrestrial, and cable broadcasting. The Kremlin is rapidly expanding RT's availability around the world and giving it a reach comparable to channels such as Al Jazeera English. According to Simonyan, the United Kingdom and the United States are RT's most successful markets.   RT does not, however, publish audience information.

- (U) According to market research company Nielsen, RT had the most rapid growth (40 percent) among all international news channels in the United States over the past year (2012). Its audience in New York tripled and in Washington DC grew by 60% (*Kommersant*, 4 July).
- (U) RT claims that it is surpassing Al Jazeera in viewership in New York and Washington DC (*BARB*, 20 November; RT, 21 November).
- (U) RT states on its website that it can reach more than 550 million people worldwide and 85 million people in the United States; however, it does not publicize its actual US audience numbers (RT, 10 December).

(U) Formal Disassociation From Kremlin Facilitates RT US Messaging

(U) RT America formally disassociates itself from the Russian Government by using a Moscow-based autonomous nonprofit organization to finance its US operations. According to RT's leadership, this structure was set up to avoid the Foreign Agents Registration Act and to facilitate licensing abroad. In addition, RT rebranded itself in 2008 to deemphasize its Russian origin.

- (U) According to Simonyan, RT America differs from other Russian state institutions in terms of ownership, but not in terms of financing. To disassociate RT from the Russian Government, the federal news agency RIA Novosti established a subsidiary autonomous nonprofit organization, TV-Novosti, using the formal independence of this company to establish and finance RT worldwide (Dozhd TV, 11 July).
- (U) Nikolov claimed that RT is an "autonomous noncommercial entity," which is "well received by foreign regulators" and "simplifies getting a license." Simonyan said that RT America is not a "foreign agent" according to US law because it uses a US commercial organization for its broadcasts (*AKT,* 4 October; Dozhd TV, 11 July).
- (U) Simonyan observed that RT's original Russia-centric news reporting did not generate sufficient audience, so RT switched to covering international and US domestic affairs and removed the words "Russia Today" from the logo "to stop scaring away the audience" (*Afisha*, 18 October; *Kommersant*, 4 July).
- (U) RT hires or makes contractual agreements with Westerners with views that fit its agenda and airs them on RT. Simonyan said on the pro-Kremlin show "Minaev Live" on 10 April that RT has enough audience and money to be able to choose its hosts, and it chooses the hosts that "think like us," "are interested in working in the anti-mainstream," and defend RT's beliefs on social media. Some hosts and journalists do not present themselves as associated with RT when interviewing people, and many of them have affiliations to other media and activist organizations in the United States ("Minaev Live," 10 April).

(U) Annex B

[redacted] Moscow's Efforts To Manipulate Foreign Elections, 2000-16

[redacted] Moscow uses a diverse toolkit of overt and covert measures to try to influence elections abroad by denigrating opponents and manipulating the election process. Moscow since at least 2000 has tried to influence elections in what it views as its sphere of influence, more recently broadening its efforts to include Europe. This chart and map below highlight examples of election manipulation with evidence of a direct link to Moscow.

(U) RUSSIA'S TOOLBOX

[redacted] We have identified six primary tools that Moscow uses to manipulate foreign elections; Russian officials base tool use on a variety of factors, including geographic distance and Russia's levers of influence in the region.

[redacted]

LOCATION OF INFLUENCE

🟥 Eurasia 🟦 West-Central Europe

MEASURE

Advisers
Providing advisers to assist in campaigning

Cyber
Deploying technical cyber capabilities to influence an election

Economic levers
Using import/export restrictions, worker visas, or energy resources to influence an election

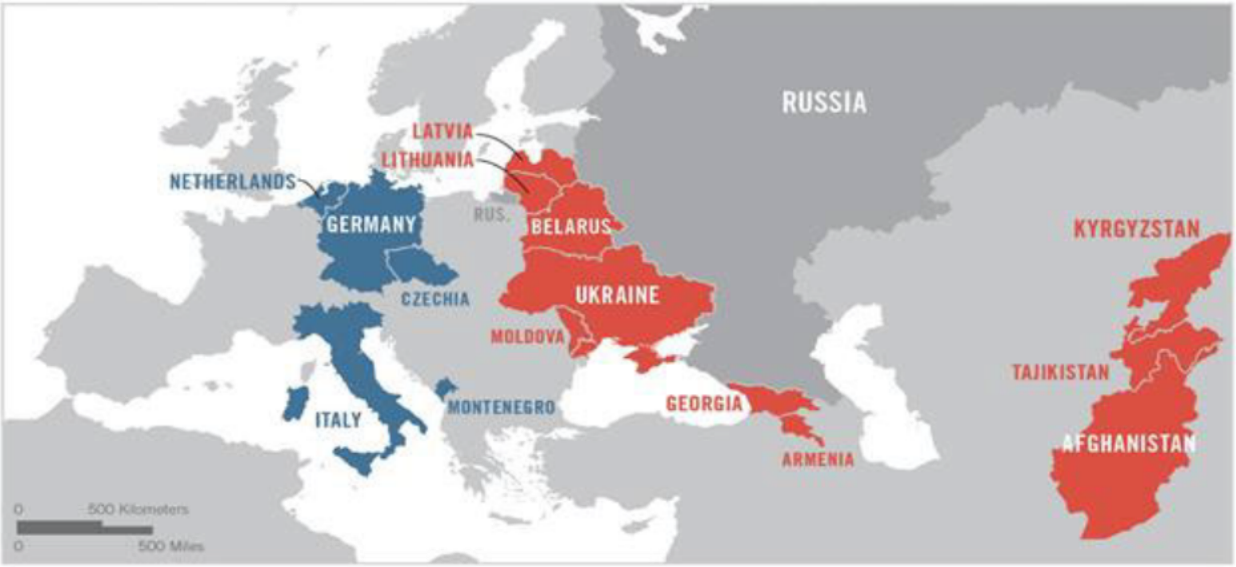
Funding
Providing money to campaigns or candidates

Messaging
Using media to promote a candidate, spreading disinformation, or releasing compromising information

Public backing
Sponsoring candidates' travel to Moscow or expressing public support for candidates

[redacted]

2000 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18



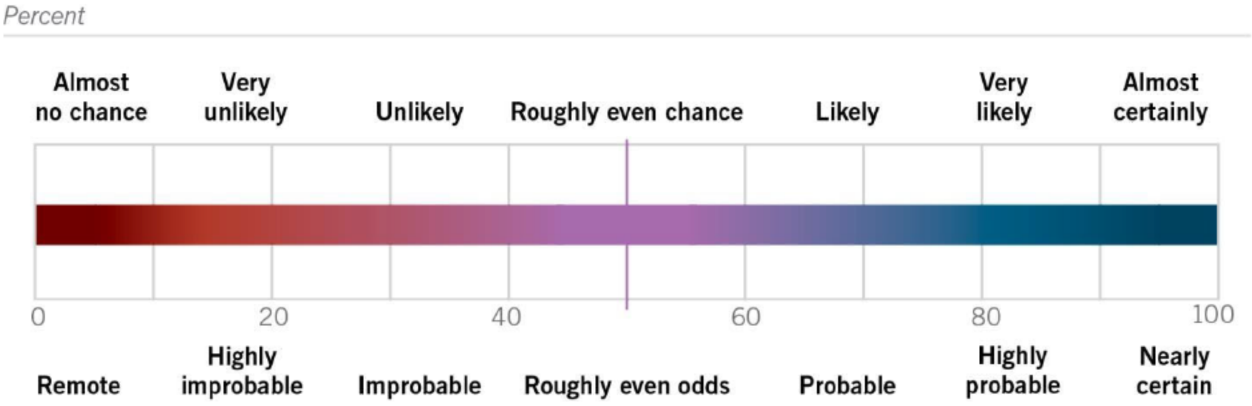
[redacted] [redacted]

(U) Annex C

(U) ESTIMATIVE LANGUAGE

(U) Estimative language consists of two elements: judgments about the likelihood of developments or events occurring and levels of confidence in the sources and analytic reasoning supporting the judgments. Judgments are not intended to imply that we have proof that shows something to be a fact. Assessments are based on collected information, which is often incomplete or fragmentary, as well as logic, argumentation, and precedents.

(U) **Judgments of Likelihood.** The chart below approximates how judgments of likelihood correlate with percentages. Unless otherwise stated, the Intelligence Community's judgments are not derived via statistical analysis. Phrases such as "we judge" and "we assess"—and terms such as "probable" and "likely"—convey analytical assessments.



(U) **Confidence in the Sources Supporting Judgments.** Confidence levels provide assessments of the quality and quantity of the source information that supports judgments. Consequently, we ascribe high, moderate, or low levels of confidence to assessments:

- (U) **High confidence** generally indicates that judgments are based on high-quality information from multiple sources. High confidence in a judgment does not imply that the assessment is a fact or a certainty; such judgments might be wrong.
- (U) **Moderate confidence** generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
- (U) **Low confidence** generally means that the information's credibility and/or plausibility is uncertain, that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that reliability of the sources is questionable.

[redacted]

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
NATIONAL INTELLIGENCE COUNCIL

[redacted]

[redacted]

```
Classification: [redacted]

[redacted]
Derived From: [redacted]
Declassify On: [redacted]
======================================================
```

From: [redacted]-DNI-[redacted]@dni[redacted]
Sent: Thursday, September 19, 2019 11:08 AM
To: [redacted]-DNI-[redacted]@dn[redacted]
Subject: RE: ACTION REQUIRED: FOIA Search DF-2019-00269 (Hermann)[redacted]

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
======================================================
```

I think you just need to respond to the request based on a plain reading of what it is asking. If you have further questions about what is responsive, I think we can link you to the FOIA officers and they probably have better expertise to guide you. Obviously, this all predates me.

On #3, it is routine that we get material and don't share it with everyone—and it's not a matter of a particular clearance.

From: [redacted]-DNI-[redacted]@dni[redacted]
Sent: Thursday, September 19, 2019 10:57 AM
To: [redacted]-DNI-[redacted]@dni[redacted]
Subject: RE: ACTION REQUIRED: FOIA Search DF-2019-00269 (Hermann)[redacted]

```
Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
======================================================
```

(U/[redacted]) I'll cut to the chase, saving detail for in–person if you think needed.

1. You DO have at least one NIC person who has been here through the whole period, & worked on the paper – me.

2. I have at least one email I'll send to [redacted]. It is a complete snoozer – OSINT based, but technically a match.

3. IF the Dossier material WAS used by the NIC, *unless* it is also compartmented, my NIO intentionally deceived and excluded me from things I was cleared for and had need to know, throughout his entire tenure here. I prefer to think that isn't true, but if it was, we have a problem.

4. IF instead, Shelby or [redacted] are mis-speaking about what the NIC was considering in its' analyses, it's a pretty reckless idea to fling out in an FOUO email.

[redacted]

From: [redacted]-DNI-[redacted]@dn[redacted]
Sent: Thursday, September 19, 2019 8:55 AM
To: [redacted]-DNI-[redacted]@dni.[redacted]
Subject: RE: ACTION REQUIRED: FOIA Search DF-2019-00269 (Hermann)[redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted], are you asking for any guidance or action by me, or is this just informational?

From: [redacted]-DNI-[redacted]@dni[redacted]
Sent: Wednesday, September 18, 2019 10:01 PM
To: [redacted]-DNI-[redacted]@dni.[redacted]
Subject: RE: ACTION REQUIRED: FOIA Search DF-2019-00269 (Hermann)[redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
===

[redacted],

(U) To you only at this time;

(U) First - when I search all my mail highside items, only 9 hits match ("steele" + "dossier") and I believe these are 1 error plus 8 open-side news compilations sent to me as a member of a wide distro. Only one of those is as old as 2017 {attached}. I can also run lowside if needed. However, because I am under unresolved Congressional retention orders regarding Russia and Elections, preventing deletion of anything Russia/Election related, I have thousands of emails on both systems that might 'hit' on wider search terms, and a sort through them is impractical.

[redacted] Second, regarding the email below – I am choosing my words carefully, for your awareness, because the premise of the message is concerning:

- As you know, I was a Deputy on the NIO Cyber team, also the de-facto elections team, from 2015 through this year

- [redacted]

- [redacted]

- [redacted]

- I have intermittently participated in IC foreign influence and election security efforts from 2014 through this evening

- I was asked by NIO Cyber [[redacted]] to participate in the analytic scrub of the non-compartmented version of what I think is the 2017 ICA referenced below. It included **no** dossier reference that I recall.
    - I was not / am not in all of the Russia compartments, and so I did not participate in the crafting of the compartmented version
    - At no point did [redacted] suggest that there was any analytically significant reporting that I was NOT seeing, with the exception of compartmented material (I asked repeatedly, because of analytic concerns I held regarding a KJ that remain unresolved to this day.)
    - At no point did I see or consider what I gather is, or was represented to be, 'dossier' materials.

- I did hear second hand from [redacted], ostensibly recounting words of then DNI Clapper, on the day of a briefing to current [then, I think, just elect] POTUS, about inclusion of dossier materials in a presentation to POTUS elect. This was characterized as an unexpected and unwanted sudden and unilateral act by then DIR FBI Comey, and as a source of concern to the DNI.

- To this day, I have never seen or reviewed dossier materials in a work setting. I did recently hear them referenced by two colleagues in terms consistent with the email below, which struck me as concerning and at odds with my personal experience working election issues during 2015-2017.

    - With that single, recent exception, other than the email below, at no time in my IC career has ‘dossier’ material ever been represented to me in a work setting as something the NIC viewed as credible, or that was influential in crafting NIC products.

[redacted] Bottom line – though I am glad to have been spared exposure to the material, if it ***was*** influential, I hope it was in a compartment I am not in, because otherwise – given my 5 years of working these topics at PDB and ICA level, to include the TS//SCI version of what I believe to be the ICA referenced - we may have a different information issue.

(U) Respectfully,

[redacted]

From: [redacted]-DNI-Y-[redacted]@dni.[redacted] **On Behalf Of** [redacted]
[redacted]
Sent: Wednesday, September 18, 2019 6:49 PM
To: [redacted]
Cc: [redacted]
Subject: ACTION REQUIRED: FOIA Search DF-2019-00269 (Hermann)

```
Classification: UNCLASSIFIED//[redacted]
===================================================
```

Election Group,

Suspense: COB Tuesday, 9/24 to NIC-Tasker

Shelby believes this should be responded to by the NIC as the dossier was a factor in the 2017 ICA on the election interference in which an assessment of the document was added as an annex.

Please review the attach document and conduct a search for the time period May 2016 through February 2017 of all records of communication (including emails on both .gov and non-.gov accounts, text messages, and instant chats) between the office of the Director of National Intelligence, including but not limited to former ODNI Director James Clapper, and the office of the Director of the Federal Bureau of Investigation, including but not limited to former FBI Director James Comey, regarding the collection of memos known as the "Steele Dossier."

Recommended search terms the “Steele” “Dossier” “Cater Page” “James Comey” and “James

Clapper" "John Brennan" in my election-related files.

Thanks,
[redacted]

[redacted]
Analytic Program Manager
[redacted]
Contractor support to the National Intelligence Council
ODNI | DDII | NIC FO
[redacted]@dni.[redacted]
[redacted]

From: [redacted]-DNI-Y-[redacted]@dni.[redacted] **On Behalf Of** [redacted]
[redacted] [redacted] September 18, 2019 2:32 PM
To: [redacted]; [redacted]
[redacted]
Cc: [redacted]
Subject: FW: ACTION REQUIRED: FOIA Search DF-2019-00269 (Hermann)

Classification: UNCLASSIFIED
===

Attn: NIMC, NIC
Suspense to MI Taskers: 1600, 24 Sep 2019
Action: See FOIA request attached and below. Provide responsive documents **and** who searched, where they searched, and what they searched for; **OR** a statement claiming your organization does not reasonably expect to have responsive documents.

[redacted]
Directorate of Mission Integration
Office of the Director of National Intelligence
Task Manager [redacted]

[redacted]

From: [redacted]-DNI-Y-[redacted]@dni[redacted]
Sent: Wednesday, September 18, 2019 2:02 PM
To: [redacted]; [redacted]
[redacted]
Cc: [redacted]-DNI-[redacted]@dni[redacted]; [redacted]-DNI-[redacted]@dn[redacted]; [redacted]-DNI-[redacted]@dni[redacted]; [redacted]-DNI-[redacted]@dni[redacted]
Subject: ACTION REQUIRED: FOIA Search DF-2019-00269 (Hermann); due COB 25 September 2019

Classification: UNCLASSIFIED

==

Good Afternoon MI and NCSC Colleagues,

The IMD/FOIA Branch received a FOIA request from Kimberly Hermann, **FOIA case DF-2019-00269,** which is now in litigation in the United Stated District Court for the Northern District of Georgia, Atlanta Division, as **Civil Action 19-cv-03144**.

Please review the attached request. If, after reviewing the attached request, you are unclear of what is being asked for, or need assistance formulating your search, reach out to the FOIA branch. We recommend utilizing the search terms 'Steele dossier' and 'Steele report' from 1 May 2016 through 28 February 2017.

Search all places likely to contain responsive documents including **both classified and unclassified emails systems; classified and unclassified user and shared drives**. Whether or not you find documents, **include information about who searched, where they searched, and what they searched for, including any search terms used.** Please ensure this tasking is forwarded to the NIC as well as any other component of MI that may reasonably have documents.

Please let us know if there are other components we should search.

As potential custodians for documents responsive to this subject, we are asking for those directly involved in work pertaining to the subject of the request to search.

All documents potentially responsive to the request must be provided to the FOIA office regardless of level of classification. The FOIA office will appropriately handle sensitive information. If you have concerns, please raise them with the FOIA office when you share the documents you have found.

Please respond to the CC'd FOIA team members and myself NLT COB **September 25, 2019.**

Contact FOIA directly with any questions or concerns.

If you feel this request is too burdensome/voluminous to process, provide information that supports your decision, along with any recommendations that would help narrow the request asap. We will attempt to negotiate with the requester.

Respectfully,

[redacted]
Freedom of Information Act Branch
Office of the Director of National Intelligence
Office: [redacted]
Secure: [redacted]

```
======================================================
Classification: UNCLASSIFIED

======================================================
Classification: UNCLASSIFIED

==============================    ====================
Classification: UNCLASSIFIED//[redacted]

================              ========================
Classification: [redacted]

================              ========================
Classification: [redacted]

================              ========================
Classification: [redacted]

================              ========================
Classification: [redacted]

================              ========================
Classification: [redacted]

================              ========================
Classification: [redacted]

================              ========================
Classification: [redacted]

================              ========================
Classification: [redacted]

================              ========================
Classification: [redacted]
```