

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

Ms. Tamara A. Johnson  
Acting Inspector General  
Intelligence Community  
Reston 3 Room E220  
Washington, D.C. 20511

Dear Acting Inspector General Johnson:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program within the Intelligence Community (IC), to include an assessment of any vulnerabilities created or exacerbated by the IC's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese government hackers

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Intelligence Community FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to IC networks, including those facilitated by VPNs and/or virtual network controllers;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the IC, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to IC networks, including the extent to which the IC has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The IC's adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the IC's chief information officer and all component chief information officers implemented additional security policies in response to COVID-19-related telework and how they are enforcing those policies; and
- Whether the IC has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

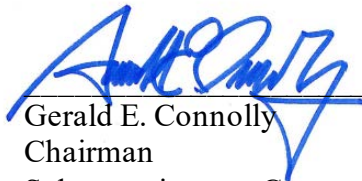
Sincerely,



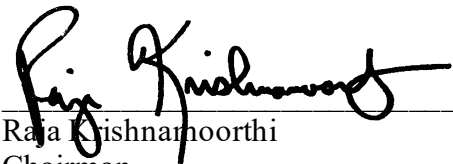
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security




Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations




Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).

  
Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties

  
Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

Ms. Diana Shaw  
Acting Inspector General  
Department of State  
PO Box 9778  
Arlington, VA 22209

Dear Acting Inspector General Shaw:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of State, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese government hackers

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Department of State FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department’s adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the Department’s chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

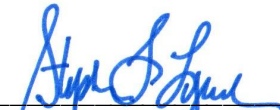
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

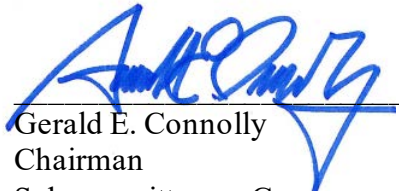
Sincerely,



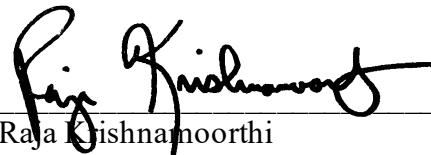
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security



Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations



Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).



Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties



Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency



**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

The Honorable Sean O'Donnell  
Acting Inspector General  
Department of Defense  
4800 Mark Center Drive  
Arlington, VA 22350

Dear Acting Inspector General O'Donnell:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of Defense (DOD), to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup> Such a review would supplement your office's previous work, which examined how DOD components secured their information technology networks during the Department's allowance of maximum telework flexibilities during the coronavirus pandemic.<sup>3</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>4</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. § 3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Department of Defense Office of Inspector General, *Audit of Maintaining Cybersecurity in the Coronavirus Disease – 2019 Telework Environment* (Mar. 29, 2021) (online at [www.dodig.mil/reports.html/Article/2556226/audit-of-maintaining-cybersecurity-in-the-coronavirus-disease-2019-telework-env/](http://www.dodig.mil/reports.html/Article/2556226/audit-of-maintaining-cybersecurity-in-the-coronavirus-disease-2019-telework-env/)).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure

(CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>5</sup> *The Washington Post* reported that “Chinese government hackers are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>6</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>7</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>8</sup>

To that end, as part of your annual DOD FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;

---

Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>5</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an “active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.”).

<sup>6</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, *Washington Post* (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](http://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>7</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;
- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department's adherence to Trusted Internet Connection 3.0 guidance;<sup>9</sup>
- Whether the Department's chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

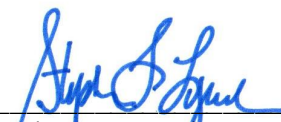
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

Sincerely,



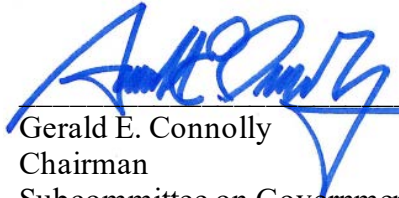
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security

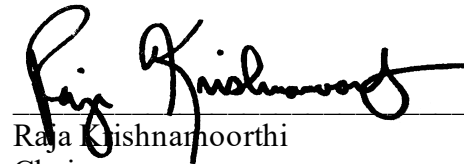
---

<sup>9</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).



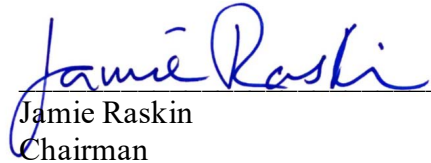
---

Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations




---

Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy



---

Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties



---

Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

The Honorable Joseph Cuffari  
Inspector General  
Department of Homeland Security  
245 Murray Drive, Building 410  
Washington, D.C. 20528

Dear Inspector General Cuffari:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of Homeland Security, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese government hackers

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Department of Homeland Security FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department's adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the Department's chief information officer and all component chief information officers implemented additional security policies in response to coronavirus<sup>9</sup>-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

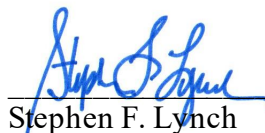
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

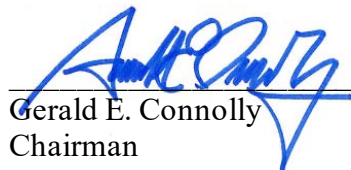
Sincerely,



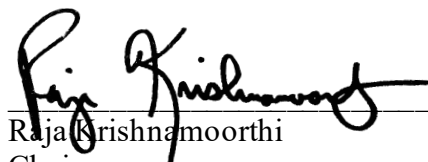
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security



Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations



Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).



Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties



Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency



**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

The Honorable Michael E. Horowitz  
Inspector General  
Department of Justice  
950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530

Dear Inspector General Horowitz:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of Justice, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese government hackers

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Department of Justice FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department’s adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the Department’s chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

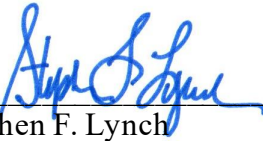
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

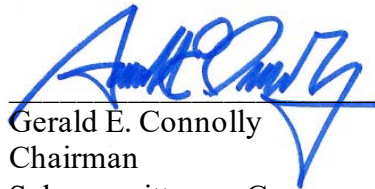
Sincerely,



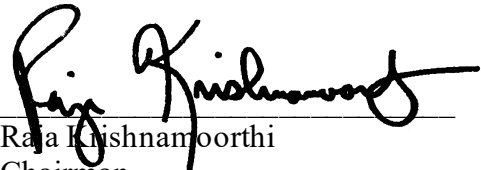
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security




Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations




Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).

  
Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties

  
Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

The Honorable Teri L. Donaldson  
Inspector General  
Department of Energy  
1000 Independence Avenue, S.W.  
Washington, D.C. 20585

Dear Inspector General Donaldson:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of Energy, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese government hackers

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Department of Energy FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department’s adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the Department’s chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

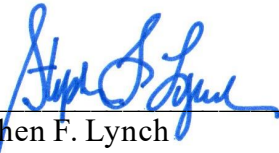
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

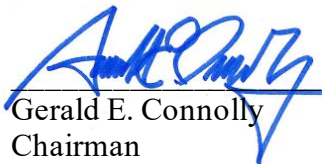
Sincerely,



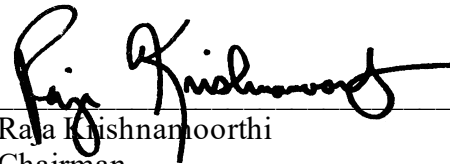
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security




Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations




Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).

  
Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties

  
Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency



**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

Mr. Richard K. Delmar  
Acting Inspector General  
Department of the Treasury  
1500 Pennsylvania Avenue, N.W.  
Washington, D.C. 20220

Dear Acting Inspector General Delmar:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of the Treasury, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) confirmed an announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

government hackers are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Department of the Treasury FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers ;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

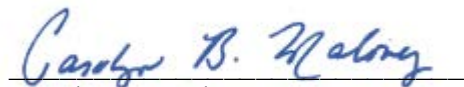
<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department’s adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the Department’s chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

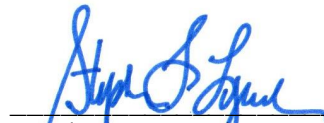
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

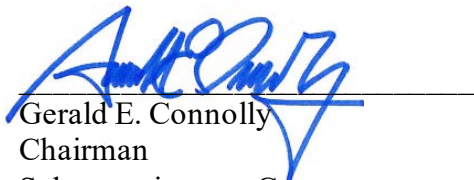
Sincerely,



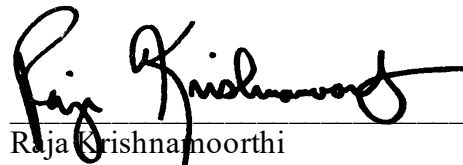
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security



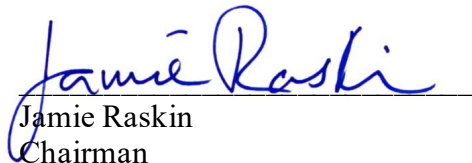
Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations



Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).



Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties



Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

Ms. Christi Grimm  
Acting Inspector General  
Department of Health and Human Services  
330 Independence Avenue, S.W.  
Washington, D.C. 20201

Dear Acting Inspector General Grimm:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of Health and Human Services, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese government hackers

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Department of Health and Human Services FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).


<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department’s adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the Department’s chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

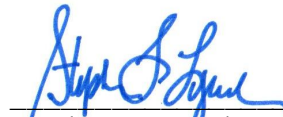
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

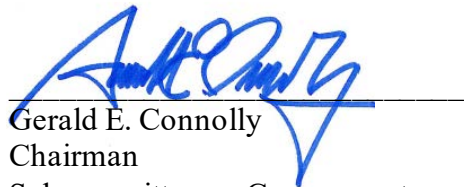
Sincerely,



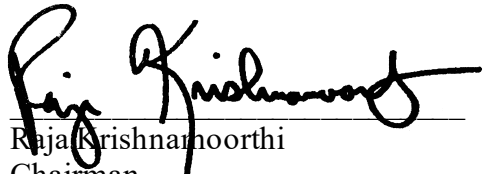
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security




Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations



Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).



---

Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties



---

Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency



**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

The Honorable Michael J. Missal  
Inspector General  
Department of Veterans Affairs  
810 Vermont Avenue, N.W.  
Washington, D.C. 20420

Dear Inspector General Missal:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of Veterans Affairs, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese government hackers

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Department of Veterans Affairs FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department’s adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the Department’s chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

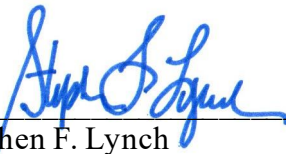
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

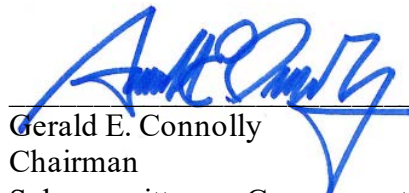
Sincerely,



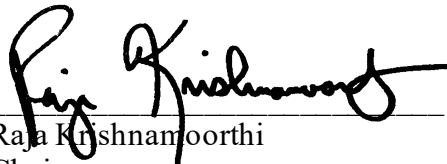
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security




Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations



Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy


---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).



---

Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties



---

Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

June 2, 2021

Ms. Sandra Bruce  
Acting Inspector General  
Department of Education  
550 12th Street, S.W.  
Washington, D.C. 20024

Dear Acting Inspector General Bruce:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.<sup>1</sup> We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of Education, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.<sup>2</sup>

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.<sup>3</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.<sup>4</sup> *The Washington Post* reported that "Chinese government hackers

---

<sup>1</sup> Pub. L. No. 113-283 (2014); 44 U.S.C. §3555.

<sup>2</sup> According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No. 111-292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at [www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

<sup>4</sup> Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>5</sup>

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that “major security concerns” associated with telework “include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.”<sup>6</sup>

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.<sup>7</sup>

To that end, as part of your annual Department of Education FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

---

<sup>5</sup> *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at [www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac\\_story.html](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>6</sup> National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>).

<sup>7</sup> Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server>).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department’s adherence to Trusted Internet Connection 3.0 guidance;<sup>8</sup>
- Whether the Department’s chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

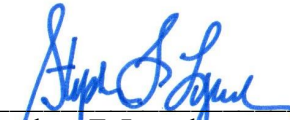
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

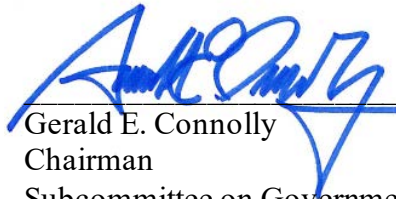
Sincerely,



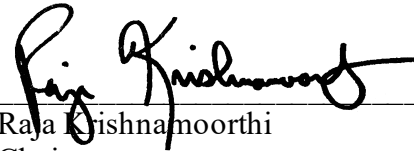
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform



Stephen F. Lynch  
Chairman  
Subcommittee on National Security




Gerald E. Connolly  
Chairman  
Subcommittee on Government  
Operations




Raja Krishnamoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

---

<sup>8</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).

  
Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties

  
Ro Khanna  
Chairman  
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member  
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

Ms. Allison C. Lerner, Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair  
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair  
Audit Committee, Council of the Inspectors General on Integrity and Efficiency