



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Ron Johnson  
Chairman  
U.S. Senate Committee on Homeland Security and Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Dear Senator Johnson:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security  
The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security  
The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science  
The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science  
The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations  
The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations  
The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations  
The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD  
WASHINGTON, D.C. 20427

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

January 6, 2016

The Honorable Jose Serrano, Ranking Member  
House Committee on Appropriations,  
Financial Services and General Government Subcommittee  
1016 Rayburn House Office Building  
Washington, DC 20515

Dear Representative Serrano:

I am grateful to you and your staff for your assistance with the FY 2016 appropriations for the Privacy and Civil Liberties Oversight Board (PCLOB). (b) (6) was extremely helpful to us throughout the process, and we are appreciative that our FY 2016 funding will help us to accomplish our agency's important mission.

PCLOB staff and I look forward to continuing to work with you as the FY 2017 process begins.

Thank you again.

Sincerely,

David Medine  
Chairman



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Nita M. Lowey  
Ranking Member  
U.S. House of Representatives Committee on Appropriations  
H-307, The Capitol  
Washington, DC 20515

Dear Representative Lowey:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security  
The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security  
The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science  
The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science  
The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations  
The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations  
The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Michael McCaul  
Chairman  
U.S. House of Representatives Committee on Homeland Security  
H2-176 Ford House  
Washington, DC 20515

Dear Representative McCaul:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget

The Honorable Jeh Johnson, Secretary, Department of Homeland Security

The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office

The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives  
Committee on Homeland Security

The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science

The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives  
Committee on Science

The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and  
Governmental Affairs

The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security  
and Governmental Affairs

The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and  
Transportation

The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and  
Transportation

The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on  
Appropriations

The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on  
Appropriations

The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations

The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD  
WASHINGTON, D.C. 20427

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

January 6, 2016

The Honorable Barbara A. Mikulski  
Vice Chairwoman, US Senate Committee on Appropriations  
S-146A, The Capitol  
Washington, DC 20510

Dear Senator Mikulski:

I am grateful to you and your staff for your assistance with the FY 2016 appropriations for the Privacy and Civil Liberties Oversight Board (PCLOB). (b) (6) and her staff were extremely helpful to us throughout the process, and we are appreciative that our FY 2016 funding will help us to accomplish our agency's important mission.

PCLOB staff and I look forward to continuing to work with you as the FY 2017 process begins.

Thank you again.

Sincerely,

David Medine  
Chairman



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Barbara Mikulski  
Vice Chairwoman  
U.S. Senate Committee on Appropriations  
S-128, The Capitol  
Washington, DC 20510

Dear Senator Mikulski:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science

The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science

The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations

The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations

The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Bill Nelson  
Ranking Member  
U.S. Senate Committee on Commerce, Science and Transportation  
512 Dirksen Senate Building  
Washington, DC 20510

Dear Senator Nelson:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security  
The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security  
The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science  
The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science  
The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations  
The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations  
The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations  
The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD  
WASHINGTON, D.C. 20427

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

January 6, 2016

The Honorable Nita Lowey, Ranking Member  
House Committee on Appropriations,  
1016 Longworth House Office Building  
Washington, DC 20515

Dear Representative Lowey,

I am grateful to you and your staff for your assistance with the FY 2016 appropriations for the Privacy and Civil Liberties Oversight Board (PCLOB). (b) (6) as extremely helpful to us throughout the process, and we are appreciative that our FY 2016 funding will help us to accomplish our agency's important mission.

PCLOB staff and I look forward to continuing to work with you as the FY 2017 process begins.

Thank you again.

Sincerely,

David Medine  
Chairman



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Hal Rogers  
Chairman  
U.S. House of Representatives Committee on Appropriations  
H-307, The Capitol  
Washington, DC 20515

Dear Representative Rogers:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board (“PCLOB”). Pursuant to the Federal Information Security Management Act (“FISMA”) of 2002, this letter constitutes our report of the Board’s information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board’s information security program were submitted to the Department of Homeland Security’s CyberScope system for inclusion in the Office of Management and Budget’s FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer (“CISO”) in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network (“PLN”).
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget

The Honorable Jeh Johnson, Secretary, Department of Homeland Security

The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office

The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security  
The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security  
The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science  
The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science  
The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations  
The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations  
The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Lamar Smith  
Chairman  
U.S. House of Representatives Committee on Science  
2321 Rayburn House Office Building  
Washington, DC 20515

Dear Representative Smith:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science

The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations

The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations

The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations

The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Bennie G. Thompson  
Ranking Member  
U.S. House of Representatives Committee on Homeland Security  
H2-176 Ford House  
Washington, DC 20515

Dear Representative Thompson:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget

The Honorable Jeh Johnson, Secretary, Department of Homeland Security

The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office

The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security  
The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science  
The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science  
The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations  
The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations  
The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations  
The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable John Thune  
Chairman  
U.S. Senate Committee on Commerce, Science and Transportation  
512 Dirksen Senate Building  
Washington, DC 20510

Dear Senator Thune:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board (“PCLOB”). Pursuant to the Federal Information Security Management Act (“FISMA”) of 2002, this letter constitutes our report of the Board’s information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board’s information security program were submitted to the Department of Homeland Security’s CyberScope system for inclusion in the Office of Management and Budget’s FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer (“CISO”) in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network (“PLN”).
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science

The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science

The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations

The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations

The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations

The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



**One Hundred Fourteenth Congress  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515**

April 29, 2016

The Honorable David Medine  
Chairman  
Privacy and Civil Liberties Oversight Board  
301 Seventh Street SW  
Washington, DC 20417

Dear Chairman Medine:

I write to express my ongoing concerns with the Federal Bureau of Investigation's (FBI) ongoing and expansion of countering violent extremism (CVE) activities, specifically related to "Shared Responsibility Committees" (SRCs).

In November 2015, I wrote the Department of Justice (DOJ) about the need for continuous and thorough oversight of the FBI's CVE activities related to SRCs. In the four months that lapsed before I received a response, the FBI publicly launched SRCs in undisclosed locations. The FBI has described SRCs as a voluntarily group made up of law enforcement officials, mental health professionals, religious leaders, family and community members that identify potential violent extremists for intervention.

I am concerned about the privacy issues that may arise from FBI's participation, and ultimate creation, of these non-criminal committees. Referrals to the committee do not end or preclude FBI from conducting concurrent criminal investigations. Moreover, intervention leaders are not protected from becoming a part of ongoing investigations and future criminal and judicial proceedings. Little information is known about the protections, if any, allotted for the voluntary intervention leaders.

The Privacy and Civil Liberties Oversight Board is vested with two fundamental authorities: (1) To review and analyze actions the executive branch takes to protect the Nation from terrorism, ensuring the need for such actions is balanced with the need to protect privacy and civil liberties and (2) To ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.<sup>1</sup> Therefore, I ask that the Board

---

<sup>1</sup> Pub. L. 110-53 (2007)

make it priority to investigate the FBI SRCs mentioned above to determine whether they (1) are conducted within the statutory authority granted by Congress, and (2) are taking the necessary precautions to protect the privacy and civil liberties of American citizens under the Constitution.

To aid in your review, I have attached (1) my November 2015 letter to Attorney General Lynch, (2) the March 2016 response to that letter, and (3) a letter outlining the SRC process.<sup>2</sup>

I ask that any information you provide be via an unclassified report, so that the public and Congress can have a long overdue debate about these important privacy concerns. If you have any questions about this request, please contact Hope Goins, Chief Counsel of Oversight at (202) 226-2616.

Sincerely,



Bennie G. Thompson  
Ranking Member  
Committee on Homeland Security

---

<sup>2</sup> <https://theintercept.com/document/2016/04/28/fbi-letter-details-shared-responsibility-committees/>



One Hundred Fourteenth Congress  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515

November 5, 2015

The Honorable Loretta E. Lynch  
Attorney General of the United States  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington, DC 20530-0001

Dear Attorney General Lynch:

Earlier this year, the White House held a three-day summit on Countering Violent Extremism. According to the White House, the summit was an opportunity to discuss concrete steps the United States and its partners can take to develop community-oriented approaches to counter hateful extremist ideologies that radicalize, recruit, or incite violence. The White House made the decision to not invite the Director of the Federal Bureau of Investigation (FBI) because the Administration's approach to counter violent extremists is a "bottom-up approach" that is "premised on the notion that local officials and communities can be an effective bulwark against violent extremism."<sup>1</sup>

Moreover, in March 2015, the 9/11 Review Commission, in its report to the Director of the FBI, found the FBI's CVE Office's "fundamental law enforcement and intelligence responsibilities do not make it an appropriate vehicle for the social and prevention role in the CVE mission."<sup>2</sup> The Commission recommended that the primary social and prevention responsibility of the FBI's CVE mission be transferred to the Department of Homeland Security or other agencies that are more directly involved with community interaction.<sup>3</sup>

---

<sup>1</sup> "F.B.I. Chief Not Invited to Meeting on Countering Violent Extremism," Michael S. Schmidt, *The New York Times*, Feb. 19, 2015.

<sup>2</sup> *The FBI: Protecting the Homeland in the 21<sup>st</sup> Century*, Bruce Hoffman, Edwin Meese, III, and Timothy Roemer, March 25, 2015.

<sup>3</sup> *Id.*

It is troubling to see the FBI is turning a deaf ear to both the White House and the 9/11 Review Commission and not only remains in the CVE space but is pursuing programs to expand its reach into America's classrooms. This week, I learned that the FBI "is developing a Website designed to provide awareness about the dangers of violent extremist predators on the Internet, with input from students, educators and community leaders."<sup>4</sup> Reportedly, this website, called "Don't Be A Puppet" is meant to be used by teachers and students to help the FBI prevent the violent extremism of youth.<sup>5</sup> According to the *Washington Post*, teachers and students in multiple Northern Virginia school districts were invited to preview the website. The *Post* also reported that the FBI would reach out to schools to see if they were interested in using the site within classrooms.<sup>6</sup> Reports indicate that the FBI is aiming for the site to be used in civics, social studies, and government classes.<sup>7</sup>

According to the U.S. Department of Education, a common refrain from educators is that they want to work with parents and students from diverse backgrounds and cultures, and to develop a shared responsibility for children's outcomes between home and school. As a former educator, I understand a teacher may be the only person that some students can trust. Also, while a teacher may be best-positioned to notice changes in a student's behavior, it is hard to see how having that teacher participate in a Federal law enforcement program would not chill relationships with students or, for that matter, undermine a supportive learning environment. Put simply, turning teachers into intelligence gathers and investigators has questionable value as a strategy for countering terrorism or violent extremism and may actually interfere with students involved in a range of risky behavior or in crisis turning away from that one person, a teacher, who might be able to make a difference.

Though I understand that plans for the website have been temporarily suspended, it is critical that you, as the leader of the Department of Justice, give personal attention to not only this program but also to the entirety FBI's CVE activities. Knowing your commitment to the Administration's countering violent extremism efforts, it is critical that you do oversight of the FBI's CVE activities, particularly with respect to the "Don't Be A Puppet" website. The FBI is responsible to you for its operations. As such, in an effort to increase transparency and gain a clearer understanding of the legal, civil liberties, privacy, and operational implications of the FBI's CVE activities, please review the FBI's CVE activities and provide the following information by November 18, 2015:

1. A timeline, from conception to implementation of the "Don't Be A Puppet" website.
2. Copies of any Privacy Impact Assessments prepared by DOJ's Chief Privacy and Civil Liberties Officer on any of the FBI's CVE programs.

---

<sup>4</sup> "Muslim activists alarmed by the FBI's new game-like counterterrorism program for kids," Michelle Boorstein, *The Washington Post*, November 2, 2015.

<sup>5</sup> Id.

<sup>6</sup> Id.

<sup>7</sup> Id.

3. Information on the national educational organizations, education leaders, childhood development specialists, and psychologists, if any, who were consulted with respect to the development of the website.
4. The names and titles of the officials from the U.S. Department of Health and Human Services, if any, who were consulted with respect to the development of the website.
5. Information on any contractors involved in the development of the website, together with information on the scope of work that each contractor performed.
6. Information on any scientific validation studies conducted prior to November 1, 2015 on the anticipated efficacy of the website.

Additionally, please provide answers to the following questions:

1. Was the U.S. Department of Education involved in the creation of this website? If so, please provide the names and titles of individuals who gave the FBI advice and counsel on the implementation of this website. Also, please specify the nature of the involvement of such individuals.
2. Did DOJ's Chief Privacy and Civil Liberties Officer conduct a Privacy Impact Assessment on the use of the website "Don't Be A Puppet" or any other website aiming to dissuade youth from participating in violent extremist activity? If so, please provide a copy.
3. According to reports, the FBI conducted focus groups to preview the website. Please provide information on the dates, locations, and durations of each preview as well as corresponding information on the individuals or groups that participated in each preview. Also, please answer the following questions:
  - A) How did the FBI determine which groups and individuals to invite to the previews?
  - B) What groups and individuals declined to attend the previews?  
How did the FBI collect feedback from participants and what, if any, feedback was recorded?
4. Does the FBI use the Violent Extremist Risk Assessment instruments (VERA or VERA-2)? Under what circumstances does the FBI employ the VERA or VERA-2 factors? Has the FBI done any research (or contracted for research with outside entities) to evaluate the effectiveness of these instruments in the circumstances in which the FBI uses them? Were these tools used to inform or create any portions of the website?
5. It has been reported that the FBI contacted schools to see if they were interested in using the program and was aiming for it to be used in civics, social studies and government classes.

- a. If so, please provide the names and locations of each school that the FBI targeted for participation.
  - b. Also, please provide information on the schools that have agreed to participate and the number of teachers at each school that would participate.
  - c. Approximately how many students at participating schools are expected to use the site when it is introduced?
  - d. For participating schools, does the FBI envision teacher participation to be discretionary or would teachers at these schools be obligated to attend training and participate in the program?
  - e. Please provide the materials which were provided to schools who have confirmed participation or interest in the website.
  - f. It was also reported that the FBI has already showed the site to some teachers and students in Northern Virginia to get feedback. Please identify each school, including its location, where the website was viewed and any feedback that was recorded by the FBI.
6. Did the Domestic Terrorism Executive Committee have the opportunity to preview the website? If so, please provide the dates the DTEC previewed the website.
  7. Did the Assistant Attorney General for National Security preview this website? If so, please provide the dates the Assistant Attorney General previewed the website.
  8. Did the Assistant Secretary for Civil Rights at the U.S. Department of Education have the opportunity to preview the website? If so, please provide the dates the Assistant Secretary previewed the website.
  9. It has been reported that at a community meeting in October, groups were provided limited detail of the FBI's plan for "Shared Responsibility Committees". One task of the committee would be to identify youth that are prone to violent extremism.
    - A. Please provide the Chief Officer for Privacy and Civil Liberties Impact Assessment on the "Shared Responsibility Committees."
    - B. Has the Assistant Attorney General for National Security been involved in the creation or implementation of "Shared Responsibility Committees?"
    - C. Please provide the names of the child psychologists and behavior therapists that provided input to the FBI for the "Shared Responsibility Committee."

Thank you for your attention to this matter. If you have any questions about this request, please contact Hope Goins, Chief Counsel for Oversight at (202) 226-2616.

Sincerely,

A handwritten signature in blue ink that reads "Bennie G. Thompson". The signature is written in a cursive, flowing style.

Bennie G. Thompson  
Ranking Member  
Committee on Homeland Security

cc: The Honorable Arne Duncan  
Secretary  
U.S. Department of Education  
400 Maryland Avenue, SW  
Washington, DC 20202

cc: The Honorable John King  
Deputy Secretary  
U.S. Department of Education  
400 Maryland Avenue, SW  
Washington, DC 20202



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 10, 2016

The Honorable Bennie G. Thompson  
Ranking Member  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Congressman Thompson:

This responds to your letter to the Attorney General dated November 5, 2015, regarding the countering violent extremism (CVE) program of the Federal Bureau of Investigation (FBI). The Department of Justice (the Department) offers the below answers to your questions and requests. We apologize for the delay in responding to your letter.

**Request #1: A timeline, from conception to implementation of the “Don’t Be a Puppet” website.**

The website’s concept originated in October 2014. The FBI assembled its subject matter experts to translate its knowledge on the various facets of violent extremism into a website. From October 2014 through February 2015, this partnership delivered a beta version of the “Don’t Be a Puppet” website. The ensuing four months resulted in the refinement of CVE content, navigation mechanisms, links, and updated information on various components of CVE. This internal FBI review process ensured the website contained accurate, factual, and useful information for the intended target audience. At the end of this development period, the website began external review, commencing in July 2015. Since July 2015 to December 2015, a team from the FBI Office of Public Affairs and the FBI CVE office held 31 focus groups representing state and local law enforcement, nongovernmental organizations, faith-based organizations, advocacy groups, academia, public schools, and other federal partners. The focus groups were held in Washington, D.C., and in other parts of the country, including Tampa, Omaha, St. Louis, Houston, Phoenix, Minneapolis, and Detroit. This allowed a cross section of society and community partners the opportunity to provide critical feedback on its development and have input into the final content. This process also ensured the FBI validated the effectiveness of the content from various segments of society. In addition, a number of the FBI’s CVE federal partners also reviewed it over the course of the website’s development. In December 2015, the development team began final editing of the content based on feedback received from the numerous focus groups. In January 2016, the website was posted on [fbi.gov](http://fbi.gov).

The Honorable Bennie G. Thompson  
Page Two

**Request #2: Copies of any Privacy Impact Assessments prepared by DOJ's Chief Privacy and Civil Liberties Officer on any of the FBI's CVE programs.**

No privacy impact assessment (PIA) has been prepared for any of the FBI's CVE programs at this time as no new electronic information systems or collections have been created to support those programs. With regard to the "Don't be a Puppet" website specifically, the FBI believes that a PIA is not required by law as the website is not an information technology that "collects, maintains, or disseminates information that is in identifiable form."

**Request #3: Information on the national educational organizations, education leaders, childhood development specialists, and psychologists, if any, who were consulted with respect to the development of the website.**

Approximately 1,000 people, including a mix of educational organizations, civic leaders, childhood development specialists, and psychologists were consulted and provided input on the content of the site. However, the consultations were done with an expectation of privacy, and the FBI does not believe it would be appropriate to release names of individuals or organizations.

**Request #4: The names and titles of the officials from the U.S. Department of Health and Human Services, if any, who were consulted with respect to the development of the website.**

The U.S. Department of Health and Human Services declined the FBI's offer to review the site and provide feedback.

**Request #5: Information on any contractors involved in the development of the website, together with information on the scope of work that each contractor performed.**

No contract was solicited or awarded to develop this website. The website was developed in-house by content developers assigned to the FBI Office of Public Affairs, who routinely update fbi.gov content and public awareness messaging.

**Request #6: Information on any scientific validation studies conducted prior to November 1, 2015, on the anticipated efficacy of the website.**

No scientific validation studies have been conducted on the website. The FBI has a team of trained professionals who have a long history of developing similar websites and educational tools.

**Question #1: Was the U.S. Department of Education involved in the creation of this website? If so, please provide the names and titles of individuals who gave the FBI advice and counsel on the implementation of this website. Also, please specify the nature of the involvement of such individuals.**

In November 2015, several U.S. Department of Education staff agreed to provide feedback on the website. The lead for the U.S. Department of Education in CVE matters at the time was David Esquith, Director of the Office of Safe and Healthy Students. The U.S.

Department of Education should be contacted for the listing of personnel who contributed to the feedback process.

**Question #2:** Did DOJ's Chief Privacy and Civil Liberties Officer conduct a Privacy Impact Assessment on the use of the website "Don't Be a Puppet" or any other website aiming to dissuade youth from participating in violent extremist activity? If so, please provide a copy.

No PIA has been completed regarding the website "Don't Be a Puppet" because no such PIA is required as the website does not collect, maintain, or disseminate any information in identifiable form. The website only collects the number of website "hits."

**Question #3:** According to reports, the FBI conducted focus groups to preview the website. Please provide information on the dates, locations, and durations of each preview as well as corresponding information on the individuals or groups that participated in each preview. Also, please answer the following questions:

- A. How did the FBI determine which groups and individuals to invite to the previews?
- B. What groups and individuals declined to attend the previews? How did the FBI collect feedback from participants and what, if any, feedback was recorded?

From July to December 2015, the FBI conducted 31 separate focus groups of the website totaling approximately 1,000 people. Feedback was overwhelmingly positive and many recommended the site and thought it was balanced, useful, did not target any one group, and was a valuable tool communities and schools needed immediately. The FBI sought a broad range of input from diverse groups. Because the consultations were done with an expectation of privacy, the FBI does not believe it would be appropriate to release names of individuals, organizations, or the specific records related to feedback.

**Question #4:** Does the FBI use the Violent Extremist Risk Assessment instruments (VERA or VERA-2)? Under what circumstances does the FBI employ the VERA or VERA-2 factors? Has the FBI done any research (or contracted for research with outside entities) to evaluate the effectiveness of these instruments in the circumstances in which the FBI uses them? Were these tools used to inform or create any portions of the website?

The FBI does not use VERA or VERA 2.

**Question #5:** It has been reported that the FBI contacted schools to see if they were interested in using the program and was aiming for it to be used in civics, social studies, and government classes.

- A. If so, please provide the names and locations of each school that the FBI targeted for participation.
- B. Also, please provide information on the schools that have agreed to participate and the number of teachers at each school that would participate.

- C. **Approximately how many students at participating schools are expected to use the site when it is introduced?**
- D. **For participating schools, does the FBI envision teacher participation to be discretionary or would teachers at these schools be obligated to attend training and participate in the program?**
- E. **Please provide the materials which were provided to schools who have confirmed participation or interest in the website.**
- F. **It was also reported that the FBI has already showed the site to some teachers and students in Northern Virginia to get feedback. Please identify each school, including its location, where the website was viewed and any feedback that was recorded by the FBI.**

The FBI worked with several school districts and educators, parents, and students to get feedback on the site. Because the consultations were done with an expectation of privacy, the FBI does not believe it would be appropriate to release names of organizations or individuals. The intent of the site is to elicit critical thinking by high school-aged youth. The FBI has a long history of educating communities on public safety issues—ranging from gangs and drugs to the more recent threat of cyber crimes. The FBI has sent its agents and other professionals into schools for decades to discuss these issues and to urge young people to turn away from crime. The approach for the development of this website was based on such things as the successful development and deployment of the FBI's web-based Safe Online Surfing (SOS) Internet Challenge, which teaches cyber safety and etiquette to children in the third through eighth grades. The FBI does not dictate how, or if, schools should implement the website in their curriculum. The site is designed for increased awareness of violent extremism.

**Question #6: Did the Domestic Terrorism Executive Committee have the opportunity to preview the website? If so, please provide the dates the DTEC previewed the website.**

The website was not reviewed by the Department's Domestic Terrorism Executive Committee (DTEC).

**Question #7: Did the Assistant Attorney General for National Security preview the website? If so, please provide the dates the Assistant Attorney General previewed the website?**

The Assistant Attorney General for National Security did not preview the website.

**Question #8: Did the Assistant Secretary for Civil Rights at the U.S. Department of Education have an opportunity to preview the website? If so, please provide the dates the Assistant Secretary previewed the website?**

The lead for the U.S. Department of Education in CVE matters is David Esquith, Director of the Office of Safe and Healthy Students. The U.S. Department of Education should be contacted for the listing of personnel who contributed to the feedback process.

The Honorable Bennie G. Thompson  
Page Five

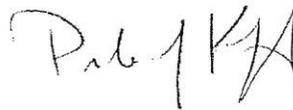
**Question #9:** It has been reported that at a community meeting in October, groups were provided limited detail of the FBI's plan for "Shared Responsibility Committees." One task of the committee would be to identify youth that are prone to violent extremism.

- A. Please provide the Chief Officer for Privacy and Civil Liberties Impact Assessment of the "Shared Responsibility Committees."
- B. Has the Assistant Attorney General for National Security been involved in the creation or implementation of "Shared Responsibility Committees?"
- C. Please provide the names of the child psychologists and behavior therapists that provided input to the FBI for the "Shared Responsibility Committee."

The FBI is in the process of rolling out a limited pilot of the Shared Responsibility Committees (SRC) concept. The committees would not be tasked with identifying youth prone to violent extremism. The Department of Justice, including the FBI, is piloting the concept to assess its viability and effectiveness.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Peter J. Kadzik  
Assistant Attorney General

cc: The Honorable Michael T. McCaul  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

cc: The Honorable Arne Duncan  
Secretary  
U.S. Department of Education  
400 Maryland Avenue, SW  
Washington, DC 20202

cc: The Honorable John King  
Deputy Secretary  
U.S. Department of Education  
400 Maryland Avenue, SW  
Washington, DC 20202



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

May 6, 2016

The Honorable Bennie G. Thompson,  
Ranking Member, Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Congressman Thompson:

Thank you for your April 29, 2016 letter regarding your ongoing concerns about the expansion of the Federal Bureau of Investigation's (FBI) activities related to countering violent extremism (CVE), and Shared Responsibility Committees (SRCs). I appreciate knowing of your interest in this matter, as well some important questions that you have raised with the U.S. Department of Justice (DoJ). I also appreciate your calling to my attention a recent press article on this topic.

As our nation's law enforcement agencies intensify efforts to combat violent extremism and homegrown terrorism, I understand the concern of many that these efforts must be balanced with the need to protect the privacy and civil liberties of law-abiding Americans. I also understand the increasing concern about privacy questions that could arise with the creation of SRCs.

As you are aware, I recently announced that I will be leaving the Privacy and Civil Liberties Oversight Board, effective July 1, 2016. The Board is currently in the process of working toward completion of its project examining counterterrorism activities conducted under Executive Order 12333. In anticipation of the completion of this work, the Board will be considering what new projects it will undertake following my departure. I have advised the Board of your request that PCLOB examine the FBI's activities related to CVE and the creation of SRCs. It is my understanding that the Board will consider this matter as a potential future examination.

I have also directed PCLOB staff to keep you and your staff advised about any developments or Board decisions with regard to this matter. Thank you again for taking the time to contact me about this important issue.

Sincerely,

A handwritten signature in cursive script that reads "David medine".

David Medine  
Chairman



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD  
WASHINGTON, D.C. 20427

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

January 6, 2016

The Honorable John Boozman, Chairman  
U.S. Senate Committee on Appropriations,  
Financial Services and General Government Subcommittee  
133 Dirksen Senate Office Building  
Washington, D.C. 20510

Dear Chairman Boozman:

I am grateful to you and your staff for your assistance with the FY 2016 appropriations for the Privacy and Civil Liberties Oversight Board (PCLOB). (b) (6) and her staff were extremely helpful to us throughout the process, and we are appreciative that our FY 2016 funding will help us to accomplish our agency's important mission: the protection of privacy and civil liberties for all Americans.

PCLOB staff and I look forward to continuing to work with you as the FY 2017 process begins.

Thank you again.

Sincerely,

David Medine  
Chairman



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Tom Carper  
Ranking Member  
U.S. Senate Committee on Homeland Security and Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Dear Senator Carper:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board (“PCLOB”). Pursuant to the Federal Information Security Management Act (“FISMA”) of 2002, this letter constitutes our report of the Board’s information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board’s information security program were submitted to the Department of Homeland Security’s CyberScope system for inclusion in the Office of Management and Budget’s FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer (“CISO”) in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network (“PLN”).
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget

The Honorable Jeh Johnson, Secretary, Department of Homeland Security

The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office

The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security  
The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security  
The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science  
The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science  
The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs  
The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation  
The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations  
The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations  
The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations  
The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Jason Chaffetz  
Chairman  
U.S. House of Representatives Committee on Oversight and Government Reform  
2157 Rayburn House Office Building  
Washington, DC 20515

Dear Representative Chaffetz:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives  
Committee on Homeland Security

The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science

The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives  
Committee on Science

The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and  
Governmental Affairs

The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security  
and Governmental Affairs

The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and  
Transportation

The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and  
Transportation

The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on  
Appropriations

The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on  
Appropriations

The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations

The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD  
WASHINGTON, D.C. 20427

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

January 6, 2016

The Honorable Thad Cochran, Chairman  
U.S. Senate Committee on Appropriations  
Room S-128,  
The Capitol  
Washington, D.C. 20510

Dear Chairman Cochran:

I am grateful to you and your staff for your assistance with the FY 2016 appropriations for the Privacy and Civil Liberties Oversight Board (PCLOB). (b) (6) and her staff were extremely helpful to us throughout the process, and we are appreciative that our FY 2016 funding will help us to accomplish our agency's important mission: the protection of privacy and civil liberties for all Americans.

PCLOB staff and I look forward to continuing to work with you as the FY 2017 process begins.

Thank you again.

Sincerely,

David Medine  
Chairman



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Thad Cochran  
Chairman  
U.S. Senate Committee on Appropriations  
S-128, The Capitol  
Washington, DC 20510

Dear Senator Cochran:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget

The Honorable Jeh Johnson, Secretary, Department of Homeland Security

The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office

The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science

The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives Committee on Science

The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations

The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations

The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD  
WASHINGTON, D.C. 20427

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

January 6, 2016

The Honorable Christopher Coons, Ranking Member  
Senate Appropriations Committee,  
Financial Services and General Government Subcommittee  
125 Senate Hart Building  
Washington, DC 20510

Dear Senator Coons:

I am grateful to you and your staff for your assistance with the FY 2016 appropriations for the Privacy and Civil Liberties Oversight Board (PCLOB). (b) (6) was extremely helpful to us throughout the process, and we are appreciative that our FY 2016 funding will help us to accomplish our agency's important mission.

PCLOB staff and I look forward to continuing to work with you as the FY 2017 process begins.

Thank you again.

Sincerely,

David Medine  
Chairman



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD  
WASHINGTON, D.C. 20427

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

January 6, 2016

The Honorable Ander Crenshaw, Chairman  
House Committee on Appropriations,  
Financial Services and General Government Subcommittee  
B300 Rayburn House Office Building  
Washington, DC 20515

Dear Chairman Crenshaw:

I am grateful to you and your staff for your assistance with the FY 2016 appropriations for the Privacy and Civil Liberties Oversight Board (PCLOB). (b) (6) as extremely helpful to us throughout the process, and we are appreciative that our FY 2016 funding will help us to accomplish our agency's important mission.

PCLOB staff and I look forward to continuing to work with you as the FY 2017 process begins.

Thank you again.

Sincerely,

David Medine  
Chairman



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Elijah Cummings  
Ranking Member  
U.S. House of Representatives Committee on Oversight and Government Reform  
2157 Rayburn House Office Building  
Washington, DC 20515

Dear Representative Cummings:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"). Pursuant to the Federal Information Security Management Act ("FISMA") of 2002, this letter constitutes our report of the Board's information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board's information security program were submitted to the Department of Homeland Security's CyberScope system for inclusion in the Office of Management and Budget's FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer ("CISO") in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network ("PLN").
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives  
Committee on Homeland Security

The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science

The Honorable Eddie Bernice Johnson, Ranking Member, U.S. House of Representatives  
Committee on Science

The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and  
Governmental Affairs

The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security  
and Governmental Affairs

The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and  
Transportation

The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and  
Transportation

The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on  
Appropriations

The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on  
Appropriations

The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations

The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD  
WASHINGTON, D.C. 20427

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

January 6, 2016

The Honorable Hal Rogers, Chairman  
House Committee on Appropriations  
H-305, The Capitol  
Washington, DC 20515

Dear Chairman Rogers:

I am grateful to you and your staff for your assistance with the FY 2016 appropriations for the Privacy and Civil Liberties Oversight Board (PCLOB). (b) (6) and her staff were extremely helpful to us throughout the process, and we are appreciative that our FY 2016 funding will help us to accomplish our agency's important mission.

PCLOB staff and I look forward to continuing to work with you as the FY 2017 process begins.

Thank you again.

Sincerely,

David Medine  
Chairman



## PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

David Medine, Chairman  
Rachel L. Brand  
Elisebeth B. Collins  
James X. Dempsey  
Patricia M. Wald

February 22, 2016

The Honorable Eddie Bernice Johnson  
Ranking Member  
U.S. House of Representatives Committee on Science  
2321 Rayburn House Office Building  
Washington, DC 20515

Dear Representative Johnson:

I write as the Chairman of the Privacy and Civil Liberties Oversight Board (“PCLOB”). Pursuant to the Federal Information Security Management Act (“FISMA”) of 2002, this letter constitutes our report of the Board’s information security program and activities for the period ending September 31, 2015. Metrics and a comprehensive assessment of the Board’s information security program were submitted to the Department of Homeland Security’s CyberScope system for inclusion in the Office of Management and Budget’s FISMA Annual Report to Congress.

Established as a fully operational Executive Branch agency towards the end of FY 2013, the Board appointed a Chief Information Officer and Chief Information Security Officer (“CISO”) in June 2014 and has been conscientiously implementing Federal standards and guidelines to ensure the efficacy of our IT policies, procedures, and practices.

In 2015 the Board has significantly improved the robustness of its security architecture and in meeting federal compliance requirements. During the reporting period, the CISO conducted five major activities:

- Designed and implemented Phase 1 of the PCLOB Enterprise Information Security Architecture.
- Completed the OMB directed 30-Day Cybersecurity Sprint including PIV implementation for local login.
- Achieved Authority to Operate for Microsoft Office 365
- Continued assessment and evaluation of applicable NIST 800-53 Information System Security Controls for the PCLOB Local Network (“PLN”).
- Initiated a guidance framework to develop, codify, and enforce IT security policies, procedures and practices IAW FISMA guidelines.

Since the implementation of IT security protections in FY 15, there have not been any major cyber security incidents during this reporting period. Starting from a baseline foundation, the information security team procured and deployed web, network and software security systems

that provides a defense-in-depth strategy. The CISO intends to complete the PLN information system's security control review, finalize the incident response capability, and amplify cybersecurity threat intelligence awareness in FY 2016.

Steady progress is being made on Cyber Security Cross-Agency Priorities ("CAP") goals. The key challenges to implementing these goals within the PCLOB information security program were:

- Boundary Protection - Implementation of Trusted Internet Connection ("TIC") requirements were cost prohibitive relative to the size of the network and the overall IT budget. Mitigating controls have been put into place and the CISO continues to work with DHS and TIC/Managed Trusted Internet Protocol Services ("MTIPS") providers to integrate TIC/MTIPS capabilities in a cost effective manner.
- Continuous Monitoring - The CISO has been incrementally building Continuous Monitoring capabilities through purchases such as the asset management tool which is compliant with the Security Content Automation Protocols. PCLOB will fully implement Continuous Diagnostics and Monitoring through the DHS Continuous Diagnostics and Mitigation Program (the "CDM Program") Blanket Purchase Agreement ("BPA") using DHS funds in 4QFY16.
- Anti-Phishing and Malware Detection - The CISO has made significant progress in this area and has a robust Anti-Phishing training program. However, there are still a number of areas within this goal that will be addressed in FY16 through internal architecture efforts.

PCLOB is doing significantly well in addressing the 2015 FISMA Metrics and the Cyber Security Cross-Agency Priority (CAP) goals through continued evolution towards a robust security architecture and continued promulgation of clear information security guidance.

Sincerely,



David Medine  
Chairman

cc:

The Honorable Shaun Donovan, Director, Office of Management and Budget  
The Honorable Jeh Johnson, Secretary, Department of Homeland Security  
The Honorable Gene L. Dodaro, Comptroller General, Government Accountability Office  
The Honorable Jason Chaffetz, Chairman, U.S. House of Representatives Committee on Oversight and Government Reform  
The Honorable Elijah Cummings, Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Michael McCaul, Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Lamar Smith, Chairman, U.S. House of Representatives Committee on Science

The Honorable Ron Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Carper, Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable John Thune, Chairman, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Bill Nelson, Ranking Member, U.S. Senate Committee on Commerce, Science and Transportation

The Honorable Hal Rogers, Chairman, U.S. House of Representatives Committee on Appropriations

The Honorable Nita M. Lowey, Ranking Member, U.S. House of Representatives Committee on Appropriations

The Honorable Thad Cochran, Chairman, U.S. Senate Committee on Appropriations

The Honorable Barbara Mikulski, Vice Chairwoman, U.S. Senate Committee on Appropriations