

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

Opening Statement
Ranking Member Elijah E. Cummings

H.R. 4361, The Federal Information Systems Safeguards Act of 2016

March 1, 2016

Mr. Chairman, I strongly oppose this legislation.

As written, this legislation would give agency heads the authority to take, quote, “any action” they deem necessary to reduce or eliminate risks or weaknesses in information technology or information systems.

Let me repeat that—“any action.”

That language is dangerously overbroad.

To say this language could be subject to abuse is a gross understatement.

This bill could open the door to an agency violating other laws in the name of security.

Could “any action” include ignoring directives from the Department of Homeland Security on cyber security? Could “any action” mean violating the Privacy Act?

Could “any action” include overriding contracting requirements, the Federal Records Act, or transparency laws, such as the Freedom of Information Act and the DATA Act?

Could “any action” mean an agency can avoid required reports to Congress on cybersecurity?

Could “any action” be withholding information from an agency’s Inspector General?

The preeminent open government organization—Openthegovernment.org—opposes this legislation because it is, quote; “open to great abuse.”

This Committee should not pass this irresponsible language.

I understand that this legislation may be intended to clarify that agency heads can block web-based email on agency computers without following requirements to bargain with the local union over the impact and implementation of such a change.

There is no question that we need to protect our federal IT and information systems from cyber threats.

I strongly support that goal.

But no matter what you believe about blocking employee access to email, this bill goes so far beyond that it loses the point.

We need to investigate the impact of this bill before rushing to enact it.

This Committee has not even held a hearing to understand the impact that this overly broad bill might have on security, human rights, privacy, contracting, or transparency protections.

The Amendment in the Nature of a Substitute says that the bill does not affect the cybersecurity provisions of the 2016 Consolidated Appropriations Act.

But in technical assistance the Department of Homeland Security provided to my staff, DHS raised concerns that, even with the amendment, this bill could conflict with authorities over cybersecurity given to OMB and DHS.

And why are we exempting this one law, when questions exist about the bill's impact in many critical areas?

We can protect federal computer systems without the unnecessarily broad and reckless language included in this bill.

I hope we can work together in the future to develop language that is carefully crafted towards fulfilling that goal. Thank you, Mr. Chairman.

Contact: Jennifer Werner, Communications Director, (202) 226-5181.