EXAMINATION OF THE GAO AUDIT SERIES OF HHS CYBERSECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JUNE 20, 2018

Serial No. 115–142

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
35–126 WASHINGTON : 2019

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon
Chairman

JOE BARTON, Texas
Vice Chairman
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CARDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

GREGG HARPER, Mississippi
Chairman

H. MORGAN GRIFFITH, Virginia
Vice Chairman
JOE BARTON, Texas
MICHAEL C. BURGESS, Texas
SUSAN W. BROOKS, Indiana
CHRIS COLLINS, New York
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia
GREG WALDEN, Oregon *(ex officio)*

DIANA DEGETTE, Colorado
Ranking Member
JANICE D. SCHAKOWSKY, Illinois
KATHY CASTOR, Florida
PAUL TONKO, New York
YVETTE D. CLARKE, New York
RAUL RUIZ, California
SCOTT H. PETERS, California
FRANK PALLONE, JR., New Jersey *(ex officio)*

CONTENTS

EXAMINATION OF THE GAO AUDIT SERIES OF HHS CYBERSECURITY

WEDNESDAY, JUNE 20, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 1:00 p.m., in room 2123, Rayburn House Office Building, Hon. Gregg Harper (chairman of the subcommittee) presiding.

Present: Representatives Harper, Griffith, Brooks, Collins, Barton, Walberg, Walters, Costello, Carter, Walden (ex officio), DeGette, Castor, Tonko, Clarke, and Ruiz.

Staff Present: Jennifer Barblan, Chief Counsel, Oversight and Investigations; Karen Christian, General Counsel; Ali Fulling, Legislative Clerk, Oversight and Investigations/Digital Commerce and Consumer Protection; Jennifer Sherman, Press Secretary; Alan Slobodin, Chief Investigative Counsel, Oversight and Investigations; Peter Spencer, Professional Staff Member, Energy; Jessica Wilkerson, Professional Staff Member, Oversight and Investigations; Julie Babayan, Minority Counsel; Chris Knauer, Minority Staff Director, Oversight and Investigations; Miles Lichtman, Minority Policy Analyst; Kevin McAloon, Minority Professional Staff Member; and Samantha Satchell, Minority Policy Analyst.

OPENING STATEMENT OF HON. GREGG HARPER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MISSISSIPPI

Mr. HARPER. Good afternoon. We are here today to hold a hearing examining the ongoing GAO audit series of HHS cybersecurity programs.

Since the Committee submitted its request to GAO in 2013, GAO has performed three audits of major operating divisions within HHS. Today's hearing will provide an opportunity for the subcommittee to learn more about GAO's findings over this series of audits as well as the steps taken by HHS and its operating divisions to respond to these findings.

Given that GAO has completed three of these audits, today's hearing will also provide an opportunity to examine HHS cybersecurity roles and responsibilities. These GAO audits provide a valuable opportunity for HHS and its operating divisions to reflect on its cybersecurity capabilities and improve from one to the next. Today's hearing will allow us to explore whether or not HHS has in-

deed taken advantage of these opportunities in the way that we would hope and expect that the Department has.

Given the sensitivity of some of the findings identified by GAO, we have determined that it is appropriate for the bulk of this hearing to take place in a closed session. After opening remarks by Ranking Member DeGette, the subcommittee will vote to enter a closed session and then proceed from there.

I want to thank our witnesses for appearing today.

And I now recognize Ms. DeGette for any public comments before we vote to go into closed session.

[The prepared statement of Mr. Harper follows:]

PREPARED STATEMENT OF HON. GREGG HARPER

Good afternoon. We are here today to hold a hearing examining the ongoing GAO audit series of HHS cybersecurity programs. Since the Committee submitted its request to GAO in 2013, GAO has performed three audits of major operating divisions within HHS.

Today's hearing will provide an opportunity for the Subcommittee to learn more about GAO's findings over this series of audits, as well as the steps taken by HHS and its operating divisions to respond to these findings. Given that GAO has completed three of these audits, today's hearing will also provide an opportunity to examine HHS cybersecurity roles and responsibilities.

These GAO audits provide a valuable opportunity for HHS and its operating divisions to reflect on its cybersecurity capabilities and improve from one to the next. Today's hearing will allow us to explore whether or not HHS has indeed taken advantage of these opportunities in the way that we would hope—and expect—that the Department has.

Given the sensitivity of some of the findings identified by GAO, we have determined that it is appropriate for the bulk of this hearing to take place in a closed session.

After opening remarks by Ranking Member DeGette, the Subcommittee will vote to enter closed session and then proceed from there.

I want to thank our witnesses for appearing today, and I now recognize Ms. DeGette for any public comments before we vote to go into closed session.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Thank you, Mr. Chairman.

As you know, this committee has conducted a series of oversight work focused on cybersecurity, such as at the Department of Energy and HHS. GAO is doing critical work in testing the cyber defenses at various HHS agencies, and this report is the latest in that series.

To that end, I look forward to examining these issues in more detail in executive session and to hearing what commitments these agencies can make to address the vulnerabilities.

And, with that, I yield back.

Mr. HARPER. Ms. DeGette yields back.

The chair recognizes himself for a unanimous consent request and to offer a motion.

Because of the sensitive nature of this hearing, particularly its implications for national security, and after consultations with the minority, I will offer a motion that the subcommittee go into executive session.

I yield to the ranking member for any comments on this procedure.

Ms. DEGETTE. Thank you, Mr. Chairman.

As I stated before, given the sensitive nature of this information, I support your motion.

Mr. HARPER. The chair moves that, pursuant to clause 2(g) of rule XI of the rules of the House, the remainder of this hearing will be conducted in executive session to protect information that might endanger national security.

Is there discussion on the motion?

Seeing none, if there is no discussion, pursuant to the rule, a recorded vote is ordered. Pursuant to rule XI of the U.S. House of Representatives, this will be a roll call vote.

The clerk call the roll.

The CLERK. Mr. Griffith?

Mr. GRIFFITH. Aye.

The CLERK. Mr. Griffith votes aye.

Mr. Barton?

[No response.]

The CLERK. Mr. Burgess?

[No response.]

The CLERK. Mrs. Brooks?

Mrs. BROOKS. Aye.

The CLERK. Mrs. Brooks votes aye.

Mr. Collins?

Mr. COLLINS. Aye.

The CLERK. Mr. Collins votes aye.

Mr. Walberg?

Mr. WALBERG. Aye.

The CLERK. Mr. Walberg votes aye.

Mrs. Walters?

Mrs. WALTERS. Aye.

The CLERK. Mrs. Walters votes aye.

Mr. Costello?

[No response.]

The CLERK. Mr. Carter?

Mr. CARTER. Aye.

The CLERK. Mr. Carter votes aye.

Chairman Walden?

[No response.]

The CLERK. Ms. DeGette?

Ms. DEGETTE. Aye.

The CLERK. Ms. DeGette votes aye.

Ms. Schakowsky?

[No response.]

The CLERK. Ms. Castor?

Ms. CASTOR. Aye.

The CLERK. Ms. Castor votes aye.

Mr. Tonko?

Mr. TONKO. Aye.

The CLERK. Mr. Tonko votes aye.

Ms. Clarke?

Ms. CLARKE. Aye.

The CLERK. Ms. Clarke votes aye.

Mr. Ruiz?

Mr. RUIZ. Aye.

The CLERK. Mr. Ruiz votes aye.
Mr. Peters?
[No response.]
The CLERK. Mr. Pallone?
[No response.]
The CLERK. Chairman Harper?
Mr. HARPER. Aye.
The CLERK. Chairman Harper votes aye.
Mr. HARPER. Have all members been recorded?
The clerk will report the vote.
The CLERK. Mr. Chairman, on the vote, there were 12 ayes and 0 nays.
Mr. HARPER. The motion passes. The remainder of the hearing will be closed to the public and open only to our witnesses, to the members, and to essential staff.
We will briefly recess to clear the room.
[Whereupon, at 1:05 p.m., the subcommittee proceeded in closed session.]
[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Mr. Chairman, thank you for holding today's hearing. As you explained, we are here today to examine the state of cybersecurity at CDC, and what the findings of this audit may mean for HHS cybersecurity more broadly. However, it is important to keep in mind that the issues and potential consequences of GAO's findings at the CDC go far beyond simply deficient technical controls.

In 2013, this Committee requested that the GAO examine in detail the information security controls at four key HHS agencies—CMS, FDA, CDC, and NIH. Three of those audits are now complete, and the NIH is up next. Two years ago, upon the release of the FDA audit, the Committee had to call FDA senior leadership in a snowstorm to impress upon them to importance of closing the 165 vulnerabilities—many of them incredibly serious-identified by that GAO audit immediately.

We had hoped that the CDC audit would be better, but in many ways it is worse. Not only are there more technical recommendations—184 in this case—but they are more severe. And, nearly a quarter of them appear to be duplicative of the vulnerabilities in the FDA audit. That includes, by the way, the vulnerability that caused the Committee to call over to FDA in a snowstorm.

CDC today will discuss their efforts to date to remediate the findings cited by GAO once GAO made them aware of the various issues. I am glad that the CDC recognizes the severity of the GAO's findings, and is aggressively moving to mitigate these vulnerabilities. CDC also engaged a US-CERT "hunt" team at the Committee's request to investigate potential intrusions. When I spoke with Dr. Redfield yesterday he told me that fixing these problems is a top priority.

We have many questions that I hope we can get answers to today. For example, why did it take a third-party audit to highlight the significant dangers that CDC's information technology strategy created? Why didn't CDC recognize this danger itself? And finally, if these findings and their potential consequences were fully recognized over a year ago, why wasn't the Committee told until the release of the restricted report last month?

Chairman Harper highlighted some of the concerns around certain vulnerabilities like Finding 38, which CDC has confirmed existed in its vulnerable configuration for nearly 7 years. The implications of this finding are astounding. For nearly 7 years, Finding 38 may have allowed a remote, Internet-based attacker to access any CDC server, workstation, or other networked device, including such CDC systems as the ones on which the Federal Select Agent Platform or the Strategic National Stockpile program depend. These are serious threats with potentially grave consequences. And to make things worse, 8 other GAO findings suggest that CDC's audit and intrusion detection capabilities were, and remain, so poor that CDC may not have detected whether Finding 38 or other critical findings were leveraged to penetrate the CDC.

The severity of the findings at CDC show that we are still viewing cybersecurity as primarily a "tech" problem, when in fact we have moved far beyond that. The

vulnerabilities at CDC were not merely a missing IT control deserving of a failing audit grade, but a national security threat. And because the appropriate amount of weight was not given to that fact a year ago, we are now even less well-positioned to understand what may have happened to—or, perhaps more accurately, who got inside—CDC's networks in the nearly 7 years that the Finding 38 vulnerability existed.

I greatly appreciate the hard work of the GAO, and I know the CDC does as well. The team that has done these audits at the Committee's request does incredible work. We must not lose sight of the context in which these vulnerabilities exist. There are malicious actors that wish to cause us great harm, and have already exploited vulnerabilities across the Federal Government. This hearing is a critical step in gaining a better understanding of what happened, so that we many ensure that all parties understand the potential consequences, and we may better position ourselves to ensure that it doesn't happen again.

I want to thank our witnesses for testifying and look forward to today's discussion. Thank you, and I yield back.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
EST. 1795

June 18, 2018

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on "Examination of the GAO Audit Series of HHS Cybersecurity"

I. INTRODUCTION

The Subcommittee on Oversight and Investigations will hold a hearing on Wednesday, June 20, 2018, at 1:00 p.m. in 2123 Rayburn House Office Building. The hearing is entitled "Examination of the GAO Audit Series of HHS Cybersecurity."

This hearing will examine a series of audits that the Energy and Commerce Committee requested that the Government Accountability Office (GAO) perform on the Department of Health and Human Services (HHS) and its component agencies' cybersecurity programs.

II. WITNESSES

- Sherri Berger, Chief Operating Officer, Centers for Disease Control and Prevention;
- Suzi Connor, Chief Information Officer, Centers for Disease Control and Prevention;
- Beth Killoran, Chief Information Officer, Department of Health and Human Services; and,
- Greg Wilshusen, Director, Information Security Issues, Government Accountability Office.

III. BACKGROUND

On December 5, 2013, the Committee on Energy and Commerce requested that GAO "examine the information security controls over key computer networks at HHS agencies," to include the Centers for Medicare & Medicaid Services (CMS), the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention (CDC), and the National Institutes of Health (NIH).[1] In that request, the Committee noted that HHS and its component agencies "rely extensively on computer systems and networks" to carry out their various missions, and that "[s]ignificant harm to public health and safety could result if the agencies'

[1] Letter from the Hon. Fred Upton, the Hon. Tim Murphy, and the Hon. Joseph Pitts, H. Comm. on Energy and Commerce to the Hon. Gene Dodaro, U.S. Gov't Accountability Office. (Dec. 5, 2013) *available at* https://archives-energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/letters/120513%20GAO%20HHS%20Cyber%20letter.pdf.

computer systems, networks, and information are not adequately protected against cyber threats."[2]

GAO accepted the Committee's request and has continued to work since that time on a series of audits examining information security controls at HHS and its component agencies. This hearing will provide Members an opportunity to learn more about what GAO has found and what steps HHS and cited agencies have taken to address those findings.

For more information on this audit series and the Committee's past work on this issue, please see:

- GAO's public audit report of CMS;[3]
- GAO's public audit report of FDA;[4]
- A blog post from FDA regarding GAO's audit of FDA;[5] and,
- A blog post from the Committee regarding GAO's audit of FDA.[6]

IV. STAFF CONTACTS

Please contact Jessica Wilkerson or Alan Slobodin of the Committee staff at (202) 225-2927 with any questions.

---

[2] *Id.*
[3] HEALTHCARE.GOV – INFORMATION SECURITY AND PRIVACY CONTROLS SHOULD BE ENHANCED TO ADDRESS WEAKNESSES, U.S. GOV'T ACCOUNTABILITY OFFICE (Sep. 2014), https://www.gao.gov/products/GAO-14-871T.
[4] INFORMATION SECURITY: FDA NEEDS TO RECTIFY CONTROL WEAKNESSES THAT PLACE INDUSTRY AND PUBLIC HEALTH DATA AT RISK, GOV'T ACCOUNTABILITY OFFICE (Sep. 2016), https://www.gao.gov/products/GAO-16-513.
[5] FDA Statement from Todd Simpson, FDA Chief Information Officer (CIO) on GAO Report Regarding FDA's IT Security Program (Sep. 29, 2016), FOOD & DRUG ADMIN., https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm523150.htm.
[6] Roadmap to Strengthening Cybersecurity: Working Together to Boost Agency Protection, U.S. H. COMM. ON ENERGY AND COMMERCE (Sep. 29, 2016), https://energycommerce.house.gov/news/blog/roadmap-strengthening-cybersecurity-working-together-boost-agency-protection/.

○