ORAL ARGUMENT NOT YET SCHEDULED

No. 17-5217

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT
DATA SECURITY BREACH LITIGATION

ON APPEAL FROM A DECISION OF THE
U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

BRIEF FOR APPELLANTS NATIONAL TREASURY EMPLOYEES UNION, EUGENE GAMBARDELLA, STEPHEN HOWELL, AND JONATHON ORTINO

GREGORY O'DUDEN
General Counsel

LARRY J. ADKINS
Deputy General Counsel

PARAS N. SHAH
Assistant Counsel

ALLISON C. GILES
Assistant Counsel

NATIONAL TREASURY
EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
(202) 572-5500

Counsel for Appellants
National Treasury
Employees Union,
Eugene Gambardella,
Stephen Howell, and
Jonathon Ortino

May 10, 2018

Certificate as to Parties, Rulings, and Related Cases

(A) Parties and Amici.

The underlying district court action was a multi-district litigation involving two separate lawsuits, one of which is at issue in this appeal (No. 17-5217) and another of which is at issue in a separate appeal before this Court (No. 17-5232), as noted in the Related Cases section below.

As pertinent to this appeal, the parties in the district court proceeding were Plaintiffs National Treasury Employees Union, Eugene Gambardella, Stephen Howell, and Jonathon Ortino (collectively, NTEU Plaintiffs); and Defendant Beth F. Cobert, Acting Director, United States Office of Personnel Management.

The parties before this Court in this appeal are Appellants National Treasury Employees Union, Eugene Gambardella, Stephen Howell, and Jonathon Ortino; Appellee Jeff T.H. Pon, Director, United States Office of Personnel Management; and Amicus Electronic Privacy Information Center.

(B) Rulings Under Review.

Appellants National Treasury Employees Union, Eugene Gambardella, Stephen Howell, and Jonathon Ortino appeal to this Court two rulings contained in Judge Amy Berman Jackson's memorandum decision in In re: U.S. Office of Personnel Management Data Security Breach Litigation, 266 F. Supp. 3d 1 (D.D.C. 2017) (JA389-462).

The two rulings under review pertain to the dismissal of the NTEU Plaintiffs' complaint. The first is the district court's ruling that NTEU Plaintiffs lacked standing to bring their action (JA405-41). The second is the district court's ruling that NTEU Plaintiffs, who brought a single legal claim based upon the constitutional right to informational privacy, failed to state a claim upon which relief could be granted (JA450-55).

(C) Related Cases.

This case was previously before the U.S. District Court for the District of Columbia, as part of Case No. 15-mc-1394, which was a coordinated proceeding involving two different lawsuits, as noted above. All substantive pleadings related to this case were

filed with the district court under Case No. 15-mc-1394, though the district court docketed NTEU Plaintiffs' specific action as Case No. 15-cv-1808. Prior to being transferred to the U.S. District Court for the District of Columbia, NTEU Plaintiffs' action was before the U.S. District Court for the Northern District of California as Case No. 3:15-cv-03144. This case has not previously been before this Court.

As noted above, the underlying district court decision in this appeal contained rulings related to two lawsuits: (1) the lawsuit brought by NTEU Plaintiffs, which is the subject of this appeal; and (2) a separate lawsuit brought by other parties and involving different legal claims than NTEU Plaintiffs' lawsuit. Some of the district court's rulings pertaining to that separate lawsuit have been appealed to this Court. That appeal has been docketed as Case No. 17-5232. On October 12, 2017, this Court issued an order consolidating Case No. 17-5232 with this case.

Counsel is not aware of any other cases pending in any other court related to this action.

/s/ Paras N. Shah

PARAS N. SHAH
Assistant Counsel

NATIONAL TREASURY
EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
(202) 572-5500
paras.shah@nteu.org

Counsel for Appellants
National Treasury Employees Union,
Eugene Gambardella,
Stephen Howell, and
Jonathon Ortino

May 10, 2018

CORPORATE DISCLOSURE STATEMENT

Pursuant to Circuit Rule 26.1, the undersigned counsel hereby certifies as follows:

1. The National Treasury Employees Union (NTEU) is an unincorporated, non-profit professional organization serving as the exclusive bargaining representative of approximately 150,000 employees of the federal government pursuant to 5 U.S.C. §§ 7101-7135.

2. NTEU has no parent companies.

3. No publicly held company has any ownership interest in NTEU.

/s/ Paras N. Shah

PARAS N. SHAH
Assistant Counsel

NATIONAL TREASURY
EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
(202) 572-5500
paras.shah@nteu.org

Counsel for Appellants
National Treasury Employees Union,
Eugene Gambardella,

Stephen Howell, and
Jonathon Ortino

May 10, 2018

TABLE OF CONTENTS

Page:

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES ii

RULE 26.1 DISCLOSURE STATEMENT vi

TABLE OF AUTHORITIES xi

GLOSSARY xvi

STATEMENT OF JURISDICTION 1

PERTINENT STATUTES AND REGULATIONS 1

STATEMENT OF ISSUES 1

STATEMENT OF THE CASE 2

I. Factual Background 2

II. Procedural History 9

III. Rulings Presented for Review 10

SUMMARY OF THE ARGUMENT 10

STANDARD OF REVIEW 14

ARGUMENT 14

I. NTEU Plaintiffs Have Standing to Bring Their Claim 14

A. OPM's Indifference to Securing NTEU Plaintiffs' Inherently Personal Information Has Caused Them Injury-In-Fact 14

1. NTEU Plaintiffs Were Injured When Their Inherently Personal Information Was Stolen... .14

2. NTEU Plaintiffs Face a Substantial Risk of Future Harm Due to the OPM Data Breaches. .17

a. NTEU Plaintiffs Face A Substantial Risk of Future Identity Theft ..... .18

b. NTEU Plaintiffs Face A Substantial Likelihood of Having Their Information Stolen Again 28

B. NTEU Plaintiffs' Injuries Are Fairly Traceable to OPM's Indifference to Securing Their Deeply Personal Information ..... .31

C. Plaintiffs' Requested Relief Would Remedy Their Injuries..... 34

II. NTEU Plaintiffs Have Sufficiently Alleged A Breach Of The Constitutional Right To Informational Privacy..... .36

A. The Constitutional Right to Informational Privacy is Firmly Recognized..... .37

B. The Right Requires the Government to Protect Personal Information Entrusted to it..... 42

C. NTEU Plaintiffs Sufficiently Allege That OPM's Databases House Their Constitutionally Protected Information 50

D. NTEU Plaintiffs Sufficiently Allege that OPM's Failure to Safeguard the Protected Information, Leading to Its Taking Violated the Right..... 52

CONCLUSION 54

CERTIFICATE OF COMPLIANCE 55

CERTIFICATE OF SERVICE 57

TABLE OF AUTHORITIES

Page:

Cases:

*ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) 15-17

AFGE v. HUD, 118 F.3d 786 (D.C. Cir. 1997) 41

Afifi v. Lynch, 101 F. Supp. 3d 90 (D.D.C. 2015) 31

Am. Inst. of Certified Pub. Accountants v. IRS, 804 F.3d 1193 (D.C. Cir. 2015) 14-15

Arakawa v. Sakata, 133 F. Supp. 2d 1223 (D. Haw. 2001) 51

Ashcroft v. Iqbal, 556 U.S. 662 (2009) 14

*Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017) 10, 17-19, 21-22, 24-26, 28, 31-34

Barry v. City of New York, 712 F.2d 1554 (2d Cir. 1983) 40, 50

Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) 23

City of Los Angeles v. Lyons, 461 U.S. 95 (1983) 31

Denius v. Dunlap, 209 F.3d 944 (7th Cir. 2000) 39

Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989) 39

DeShaney v. Winnebago Cnty. Dep't of Soc. Servs., 489 U.S. 189 (1989) 48

Dieffenbach v. Barnes & Noble, Inc., 2018 U.S. App. LEXIS 9051 (7th Cir. Apr. 11, 2018) 20

Doe v. Webster, 606 F.2d 1226 (D.C. Cir. 1979) 40

*Eagle v. Morgan, 88 F.3d 620 (8th Cir. 1996) 39, 44, 50, 52

*Fadjo v. Coon, 633 F.2d 1172 (5th Cir. 1981) 42-43, 52

Ferm v. United States, 194 F.3d 954 (9th Cir. 1999) 39, 51-52

Fraternal Order of Police, Lodge 5 v. City of Philadelphia,
812 F.2d 105 (3d Cir. 1987) 50

*Galaria v. Nationwide Mut. Ins. Co.,
663 F. App'x 384 (6th Cir. 2016)..... 21-22, 25, 32

Gelboim v. Bank of Am. Corp., 135 S. Ct. 897 (2015) 27

In re Adobe Sys., Inc., Privacy Litig.,
66 F. Supp. 3d 1197 (N.D. Cal. 2014) 31, 35

In re Horizon Healthcare Servs. Data Breach Litig.,
846 F.3d 625 (3d Cir. 2017) 23

In re: SuperValu, Inc., Customer Data Sec. Breach Litig., 870
F.3d 763 (8th Cir. 2017)..... 24

In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.,
138 F. Supp. 3d 1379 (J.P.M.L. 2015) 10

In re: U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.,
266 F. Supp. 3d 1 (D.D.C. 2017) 10

*In re Zappos.com, Inc., 2018 U.S. App.
LEXIS 10031, (9th Cir. Apr. 20, 2018) 23, 34-35

J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981) 40

*James v. Douglas, 941 F.2d 1539 (11th Cir. 1991) 39, 44, 52

Jewel v. NSA, 673 F.3d 902 (9th Cir. 2011) 35

Klayman v. Obama, 142 F. Supp. 3d 172 (D.D.C. 2015) 17

Krottner v. Starbucks, Corp., 628 F.3d 1139 (9th Cir. 2010) 22, 25

La. Energy & Power Auth. v. FERC, 141 F.3d 364 (D.C. Cir. 1998) 15

*NASA v. Nelson, 562 U.S. 134 (2011) 12, 39

Nat'l Fed'n of Fed. Emps. v. Greenberg, 983 F.2d 286 (D.C. Cir. 1993) 40-41

New York v. Ferber, 458 U.S. 747 (1982) 39

Nixon v. Admin. of Gen. Servs., 433 U.S. 425 (1977) 38-39, 41

Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260 (9th Cir. 1998) 50

Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) 24

Remijas v. Neiman Marcus Grp., 794 F.3d 688 (7th Cir. 2015) 22, 35

*Sheets v. Salt Lake Cnty., 45 F.3d 1383 (10th Cir. 1995) 39, 45, 50, 52

Trudeau v. FTC, 456 F.3d 178 (D.C. Cir. 2006) 14

United States v. Hubbard, 650 F.2d 293 (D.C. Cir. 1980) 40

United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980) 40

Walls v. Petersburg, 895 F.2d 188 (4th Cir. 1990) 40

Whalen v. Michaels Stores, Inc.
689 F. App'x 89 (2d Cir. 2017)..... 24

*Whalen v. Roe,
429 U.S. 589 (1977)..... 36-43, 45-46, 49

Woodland v. City of Houston, 940 F.2d 134 (5th Cir. 1991)..... 39

Statutes:

28 U.S.C. § 1291..... 1

28 U.S.C. § 1331..... 1

44 U.S.C. § 3554..... 3

Miscellaneous:

A. Michael Froomkin, Government Data Breaches,
24 Berkley Tech. L. J. 1019 (2009)..... 48

Brief for the Petitioners, NASA v. Nelson, 2010 U.S. S. Ct. Briefs
LEXIS 448 (May 20, 2010)..... 41

Reply Brief for the Petitioners, NASA v. Nelson, 2010 U.S. S. Ct.
Briefs LEXIS 1494 (Sept. 1, 2010)..... 41

OPM: Data Breach: Hearing Before House Comm. On Oversight
and Gov't Reform, 114th Cong. (2015)..... 13

OPM OIG Office of Audits, Final Audit Report, Audit of the U.S.
Office of Personnel Management's Security Assessment and
Authorization Methodology (June 20, 2017),
https://www.opm.gov/our-inspector-general/reports/2017/audit-
of-the-us-office-of-personnel-management%E2%80%99s-

security-assessment-and-authorization-methodology-4a-ci-00-17-014.pdf 30

OPM OIG Office of Audits, Management Advisory, U.S. Office of Personnel Management's Fiscal Year 2017 IT Modernization Expenditure Plan (Feb. 15, 2018), https://www.opm.gov/our-inspector-general/management-advisory-reports/management-advisory-report-us-office-of-personnel-management%E2%80%99s-fiscal-year-2017-it-modernization-expenditure-plan.pdf 30

GLOSSARY

JA	Joint Appendix
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
IT	Information Technology
NTEU	National Treasury Employees Union
NTEU Plaintiffs	National Treasury Employees Union, Eugene Gambardella, Stephen Howell, and Jonathon Ortino
OIG	Office of Inspector General
OMB	United States Office of Management and Budget
OPM	United States Office of Personnel Management
PII	Personally Identifiable Information
PIV	Personal Identity Verification
SSN	Social Security Number

STATEMENT OF JURISDICTION

The district court had subject matter jurisdiction over the legal claim that the National Treasury Employees Union (NTEU), Eugene Gambardella, Stephen Howell, and Jonathon Ortino (collectively, NTEU Plaintiffs) raise. 28 U.S.C. § 1331. This Court has jurisdiction over this appeal of the district court's dismissal of NTEU Plaintiffs' claim. 28 U.S.C. § 1291. The district court's decision, issued on September 19, 2017, was a final judgment disposing of NTEU Plaintiffs' legal claim. JA461-62. NTEU Plaintiffs timely appealed on September 19, 2017. JA463-64.

PERTINENT STATUTES AND REGULATIONS

The relevant statutory provisions are reproduced in the addendum to this brief.

STATEMENT OF ISSUES

1. Whether the district court erred in ruling that NTEU Plaintiffs lacked standing to pursue their legal claim.

2. Whether the district court erred in ruling that NTEU Plaintiffs failed to state a claim on which relief could be granted.

STATEMENT OF THE CASE

I. Factual Background.

NTEU Plaintiffs' complaint alleges the following facts, which must be taken as true for purposes of this appeal because the district court disposed of their complaint at the pleading stage:

On June 4, 2015, the Office of Personnel Management (OPM) announced it had uncovered a data breach involving hackers downloading from OPM's databases the names, addresses, dates and places of birth, and social security numbers of approximately 4.2 million employees, including thousands of NTEU members. JA160-61(¶¶13,15,16). OPM first detected the data breach in April 2015, and it is believed to have been perpetrated in October 2014. JA160-61(¶14).

On June 12, 2015, OPM announced it had uncovered another data breach involving hackers downloading from OPM's databases the confidential background investigation materials of prospective, current, and former federal employees. JA161-62(¶¶18-19). Approximately 21.5 million individuals had their personal information exposed through this breach, including thousands of NTEU members. JA162(¶19),178-79(¶74). OPM detected the breach in May 2015, and it is believed to

have been perpetrated in July and August 2014. JA162-62(¶18). During this period, the perpetrators of this breach repeatedly accessed and took personal information from OPM's databases related to confidential background investigations that OPM has conducted. JA161-62(¶¶18-19).

The standard forms that federal employees must submit for their background investigations require them to disclose, or authorize OPM to obtain, among other information, social security numbers, criminal history, disciplinary problems, marital information (including marital problems), past drug or alcohol use, police records, financial data, and medical information (including mental health issues). JA162-65(¶¶19-32). This information was among the information exposed in the breach announced on June 12, 2015. JA162-65(¶¶19-32). OPM explicitly promised individuals submitting these forms that "the information [provided] will be protected from unauthorized disclosure." JA178(¶69); see JA177(¶¶67-68).

The Federal Information Security Management Act (FISMA), codified in pertinent part at 44 U.S.C. § 3554, tasks each agency head with safeguarding agency information systems, reducing the risk of

data breaches, and complying with technology standards and guidelines issued by appropriate entities. JA167(¶¶36-37). In its FISMA audit for fiscal year 2014, OPM's Office of Inspector General (OIG) documented numerous deficiencies in OPM's information technology security. JA168(¶41). OPM Assistant Inspector General for Audits, Michael R. Esser, testified to Congress that some of these problems dated back to fiscal year 2007. JA169(¶43). Mr. Esser testified, for example, that OPM's security governance constituted a "material weakness" for fiscal years 2007 through 2013, and a "significant deficiency" in 2014. JA169-70(¶44). A "material weakness" is a "severe control deficiency that prohibits the organization from adequately protecting its data," and a "significant deficiency" means that the technical infrastructure is "inherently difficult to protect." JA169-70(¶44).

The Office of Management and Budget (OMB) requires all federal information systems to have a valid "authorization." JA170(¶45). An "authorization" is a "comprehensive assessment of each IT system to ensure that it meets the applicable security standards before allowing the system to operate in an agency's technical environment." JA170(¶45). Mr. Esser, however, testified that eleven OPM information

systems were operating without a valid authorization. JA170(¶45). He explained that "the volume and sensitivity of OPM's systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program." JA170-71(¶46). He recommended that these systems be shut down in 2014, but OPM rejected his recommendation. JA170(¶45).

Mr. Esser further testified that the 2014 audit report revealed that "two of the most critical areas in which OPM needs to improve its technical security controls relate to configuration management and authentication of IT systems using personal identity verification (PIV) credentials" to verify employees' identities. JA171(¶47). "Configuration management" relates to the "policies, procedures, and technical controls used to ensure that IT systems are securely deployed." JA171(¶48). As of 2014, some of OPM's regular system vulnerability scans "were not working correctly because the tools did not have the proper credentials," and "some servers were not scanned at all." JA171(¶48). And, despite OMB requirements, "none of the agency's major applications" required PIV authentication, which would have required that a hacker compromise more than a username and password to access its

databases. JA172(¶50). Nor did OPM perform the basic cybersecurity practice of encrypting data. JA172-73(¶¶51-52).

Additionally, federal guidelines require agencies to develop and maintain an inventory of its information systems and to audit all activities associated with those systems. JA171-72(¶49). But OPM did not maintain an accurate centralized inventory of all servers and databases. JA171-72(¶49). "[W]ithout a comprehensive list of assets that need to be protected and monitored," Mr. Esser noted, OPM could not "fully defend its network." JA171-72(¶49).

As Mr. Esser testified, "some of the current problems and weaknesses were identified as far back as Fiscal Year (FY) 2007. We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today." JA173-74(¶54). OPM's Inspector General agreed that OPM's cybersecurity shortcomings "without question . . . exacerbated the possibility" of a breach. JA174-75(¶56).

OPM continues to ignore the longstanding recommendations of its OIG, raising the substantial likelihood of another breach. JA181-84(¶¶87-91). In its fiscal year 2015 audit report, OPM's OIG reiterated

that, "for many years, we have reported critical weaknesses in OPM's ability to manage its IT environment, and warned that the agency was at an increased risk of a data breach." JA182(¶88) (noting its "recommendations appeared to garner little attention, as the same findings were repeated year after year"). Given "the overall lack of compliance that seems to permeate the agency's IT security program," the OIG concluded that it was "very concerned that the agency's systems will not be protected against another attack." JA182(¶88).

On May 9, 2016, the vendor that OPM hired to overhaul its information technology infrastructure "abruptly ceased operations," with one month left on its contract and the status of its work unknown. JA183-84(¶90) (noting vendor's "troubled history with government contracting"). On May 18, 2016, OPM's OIG issued an interim status report, stating that, having reviewed OPM's business plan for its IT upgrades, it was "even more concerned" about OPM's plans to update its IT security because OPM failed to perform the mandatory planning steps that OMB requires for such a project and also failed to develop a "realistic budget." JA184(¶91).

Plaintiffs Eugene Gambardella, Jonathon Ortino, and Stephen Howell were federal employees who had their personal information exposed by the OPM data breaches. JA157-58(¶¶6-8),175-77(¶¶59-66), 178(¶¶71-72). All three submitted background investigation forms with personal information that they had reason to believe, based on the government's promise, would be safeguarded from unauthorized disclosure. JA177-78(¶¶66-69). Apart from the OPM data breaches, none of the three plaintiffs has had, to the best of his knowledge, his personal information exposed in any other public or private sector data breach. JA180-81(¶¶82,85-86). When the breaches occurred, all three plaintiffs lost their sense of security in the protection of their personal data. JA179(¶¶77-78),185(¶¶93-94).

In addition, in early 2016, an individual federal tax return was fraudulently filed in Mr. Gambardella's name. JA180(¶79). Mr. Gambardella had to consult with the IRS before filing his legitimate federal return. JA180(¶80). When Mr. Gambardella was finally able to re-file his 2015 federal return, the IRS required that he do so in paper form; the delay in his being able to file his legitimate return and the requirement that he file in paper form delayed his tax refund of

approximately $7,000 by several months. JA180(¶¶80-81),190-91. Because the OPM data breaches are the only data breaches that have implicated his personal information, Mr. Gambardella believes that the fraudulent federal tax return, which led to a delay in his federal tax refund, stemmed from the OPM data breaches. JA181-82(¶83).

As Mr. Gambardella's experience shows, OPM's past and continued indifference to its security obligations has put NTEU members, including NTEU's individual plaintiffs, at a substantial risk of future harm, including additional unauthorized access of their inherently personal information, in further violation of their constitutional rights, and identity theft. JA181-85(¶¶87-92).

II. Procedural History.

NTEU Plaintiffs filed a complaint against the Director of OPM in the U.S. District Court for the Northern District of California on July 8, 2015, alleging a violation of NTEU members' constitutional right to informational privacy and seeking declaratory and injunctive relief. JA156(¶2). That complaint was transferred to the U.S. District Court for the District of Columbia on October 9, 2015, for consolidated or coordinated proceedings with other actions arising from the OPM data

breaches. In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 138 F. Supp. 3d 1379 (J.P.M.L. 2015). NTEU filed an amended complaint maintaining the same cause of action on June 3, 2016. JA153-89. The district court dismissed NTEU Plaintiffs' complaint for lack of standing (JA405-41), and, alternatively, for failure to state a claim upon which relief can be granted (JA450-55).

III. Rulings Presented for Review.

NTEU Plaintiffs appeal from the memorandum opinion that the Honorable Amy Berman Jackson issued on September 19, 2017, in In re: U.S. Office of Personnel Management Data Security Breach Litigation, 266 F. Supp. 3d 1 (D.D.C. 2017) (JA389-462). Specifically, NTEU Plaintiffs appeal the district court's rulings that they lacked standing and that they failed to state a claim upon which relief can be granted. JA405-41,450-55.

SUMMARY OF THE ARGUMENT

1. Had standing been analyzed consistent with this Court's precedent, including Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), and had critical allegations not been disregarded, the district court would have concluded that NTEU Plaintiffs have standing to

bring their constitutional claim. NTEU Plaintiffs have laid out two bases for their standing.

First, NTEU Plaintiffs' standing arose the moment that their inherently personal information was stolen from OPM's deficiently secured databases. At that moment, NTEU Plaintiffs' constitutional right to informational privacy was violated and their sense of security in their personal data was lost, giving rise to an Article III injury. The district court erred by ignoring this standing argument altogether.

Second, NTEU Plaintiffs have shown that they have standing because the theft of their personal information has created an increased and substantial risk of identity theft. This Court has joined the majority view of the courts of appeals and ruled, as explained below, that where a sophisticated actor perpetrates a data breach and steals information that could be used to effect identity theft, the data breach victims are at a substantial risk of future identity theft, which is sufficient for standing. Here, it is undisputed that the OPM data breaches were perpetrated by a sophisticated, albeit unknown, hacker and that the information stolen could be used to perpetrate identity theft. The district court erred by not following this Court's precedent.

2. The district court further erred in concluding that NTEU Plaintiffs failed to state a claim based upon the constitutional right to informational privacy. The Supreme Court has indicated, and nine courts of appeals have held, that the right requires a sufficient justification from the government to collect inherently personal information from individuals. Four courts of appeals, moreover, have held that the right's protections persist even after that information is disclosed to the government.

This Court has acknowledged the right in several decisions. And not even the government has argued—in this case or in the most recent Supreme Court case on this issue, NASA v. Nelson, 562 U.S. 134 (2011)—that the right does not exist. Indeed, the government's briefs in Nelson acknowledge the right and give the government's views on its parameters.

This case should thus turn on the scope of the right's protections, not its existence. NTEU Plaintiffs' position is that the right, once recognized, must be interpreted consistent with its core purpose: protecting the confidentiality of fundamentally personal information. Consistent with that purpose, four courts of appeals have indicated that

the right is violated when the government discloses inherently personal information collected on the promise of confidentiality to third parties unauthorized to view the information. These cases show that courts of appeals, once recognizing the right, have imputed to the government an affirmative obligation not to disclose protected material that it has promised to keep confidential.

If this affirmative obligation is violated when the government intentionally discloses inherently personal information entrusted to it with the expectation of confidentiality, it must follow that the right is also violated when the government effectively leaves that information in a room with all the doors and windows open.[1] NTEU Plaintiffs have pled with sufficient specificity that OPM violated NTEU members' constitutional right to informational privacy through its reckless indifference to protecting their inherently personal information.

[1] See OPM: Data Breach: Hearing Before House Comm. on Oversight and Gov't Reform, 114th Cong. 2 (2015) ("According to the last eight years of IG reports, OPM's data security posture was akin to leaving all the doors and windows open at your house[.]") (statement of Chairman Jason Chaffetz).

STANDARD OF REVIEW

This Court reviews Rule 12 dismissals de novo. Trudeau v. FTC, 456 F.3d 178, 183 (D.C. Cir. 2006). To survive a Rule 12 motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). The Court "'must treat the complaint's factual allegations as true and must grant the plaintiff the benefit of all inferences that can be derived from the facts alleged.'" Trudeau, 456 F.3d at 193 (quotation and alteration omitted).

ARGUMENT

I. NTEU Plaintiffs Have Standing to Bring Their Claim.

The district court's standing analysis wrongly side-stepped binding precedent and pertinent factual allegations. It also ignored one of NTEU Plaintiffs' standing arguments altogether.

A. OPM's Indifference to Securing NTEU Plaintiffs' Inherently Personal Information Has Caused Them Injury-In-Fact.

1. NTEU Plaintiffs Were Injured When Their Inherently Personal Information Was Stolen.

In evaluating standing at the motion to dismiss stage, this Court "must assume that the plaintiffs state a valid legal claim." Am. Inst. of

Certified Pub. Accountants v. IRS, 804 F.3d 1193, 1196 (D.C. Cir. 2015) (quotation omitted). Thus, unless it is "entirely frivolous," the underlying legal claim must be assumed to be well-founded for a Rule 12 standing analysis. La. Energy & Power Auth. v. FERC, 141 F.3d 364, 368 (D.C. Cir. 1998).

NTEU Plaintiffs allege that their constitutional right to informational privacy was violated and that their sense of security in their data was lost when hackers stole their inherently personal information from databases that OPM irresponsibly failed to secure. JA185-86(¶¶95-98). In light of this claim, which must be accepted as valid for this standing inquiry, NTEU Plaintiffs' Article III injury arose simultaneous with that theft.

The Second Circuit's decision in ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015), illustrates NTEU Plaintiffs' standing here. There, plaintiffs challenged the constitutionality of a federal program allowing the National Security Agency to collect "metadata associated with telephone calls made by and to Americans[.]" Id. at 792. The government argued that the plaintiffs lacked standing because,

although their metadata had been collected, they could only speculate about whether the government would review that data. Id. at 800-01.

The Second Circuit examined the standing question in light of the claims asserted by the plaintiffs. Id. at 801. It concluded that "[w]hether or not such claims prevail on the merits, appellants surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them." Id. That is, the plaintiffs in Clapper had standing at the moment the allegedly wrongful act occurred: the collection of their personal metadata.

Likewise, here, NTEU Plaintiffs' injury—the violation of their constitutional right to informational privacy and their loss of security in their personal data—arose when the breach occurred. There is no dispute that there have been data breaches through which Plaintiffs Gambardella, Howell, and Ortino had inherently personal information stolen from OPM's databases, which were not adequately secured. JA157-58(¶¶6-8),160-62(¶¶13-19),167-77(¶¶36-66),178(¶¶71-72). At that moment, their rights were violated (JA179(¶76)) and their sense of security in the protection of their personal data was lost. JA179(¶¶77-78),186(¶¶93-94).

Just as the plaintiffs in ACLU v. Clapper did not need to establish, for standing purposes, that their metadata had been reviewed, neither is it required for NTEU Plaintiffs to establish that their personal information has been used in a particular way. See ACLU v. Clapper, 785 F.3d at 801-02; Klayman v. Obama, 142 F. Supp. 3d 172, 186-87 (D.D.C. 2015) (following ACLU v. Clapper standing analysis and concluding that plaintiffs' Article III injury occurred when phone data was collected), vacated as moot, 2016 U.S. App. LEXIS 6190 (D.C. Cir. Apr. 4, 2016).

The district court did not assess this argument. Its analysis instead lumped NTEU Plaintiffs' injury allegations with allegations contained in a different lawsuit raising different causes of action. See JA409-20.

2. NTEU Plaintiffs Face a Substantial Risk of Future Harm Due to the OPM Data Breaches.

This Court has "frequently upheld claims of standing based on allegations of a 'substantial risk' of future injury." Attias, 865 F.3d at 627. NTEU Plaintiffs have alleged that they are at substantial risk of two types of future harm, either of which constitutes an Article III injury. First, the sophisticated, targeted hackings that took place and

the types of information stolen put NTEU Plaintiffs at an increased and substantial risk of future harm, including identity theft. Second, OPM's continued indifference to IT security and its continued IT security deficiencies, as reported by its Inspector General, puts NTEU Plaintiffs at an increased and substantial risk of having their deeply personal information stolen again.

a. NTEU Plaintiffs Face A Substantial Risk of Future Identity Theft.

1. As explained below, in Attias, this Court joined the majority view among the courts of appeals that where—as here—a complaint alleges that a sophisticated actor has perpetrated a data breach that exposed the types of information that can be used to steal the victims' identities, those victims have sufficiently pled an Article III injury. The district court side-stepped this binding, on-point authority, and its ruling should be reversed.

In Attias, this Court explained how to assess whether data breach victims have sufficiently pled an Article III injury based on a "substantial risk of future harm" theory. See 865 F.3d at 627. The central question, "keeping in mind the light burden of proof the plaintiffs bear at the pleading stage, is whether the complaint plausibly

alleges that the plaintiffs now face a substantial risk of identity theft as a result of . . . the data breach." Id.

Attias's discussion of the types of allegations that are sufficient, at the motion to dismiss stage, to adequately plead an Article III injury under this "substantial risk" of future harm approach, confirms that NTEU Plaintiffs have done so here. Attias concluded that the plaintiffs sufficiently alleged an Article III injury where they alleged that the breached entity stored sensitive personal information, including social security and credit card numbers; that this sensitive information was stolen in the data breach at issue; and that the theft of the data put them "at a high risk of financial fraud." Id. at 628. Based upon these allegations, the Court concluded that "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken," satisfying Article III's injury-in-fact requirement. Id. at 629.

NTEU Plaintiffs have alleged, similarly, that their social security numbers and other highly personal information were stored on OPM's databases; that their sensitive information was stolen by sophisticated hackers who targeted the information and repeatedly breached OPM's

databases to take it; and that the theft of that data has put NTEU Plaintiffs at substantial risk of future harm, such as identity theft. JA157-58(¶¶6-8),160-65(¶¶13-32),175-77(¶¶59-66),178(¶¶71-72),181-85(¶¶87-92).

And, illustrating the substantial risk of future harm, NTEU Plaintiffs have alleged that Plaintiff Gambardella has already suffered identity theft attributable to the OPM data breaches. Plaintiff Gambardella had a false tax return filed in his name following the OPM data breaches that he reasonably attributes to the data breaches. JA180-81(¶¶79-83). The fraudulent tax return was filed after OPM data breaches occurred, and Mr. Gambardella's personal information has not been exposed in any other data breach. JA180-81(¶¶79-83).

Mr. Gambardella suffered financial harm due to the fraudulent return; although he eventually received his tax refund of approximately $7,000, he lost use of those funds for several months. JA180(¶81),190-91. This temporary loss qualifies as an Article III injury. See Dieffenbach v. Barnes & Noble, Inc., 2018 U.S. App. LEXIS 9051, at *3-5 (7th Cir. Apr. 11, 2018) (rejecting the view, embraced by the district court below, JA422-23, that, in the data breach context, economic loss is

required to show Article III injury). So too does the time and effort that Mr. Gambardella spent "sorting things out" (see id.) with the IRS after he discovered the fraudulent filing. JA180(¶80).

NTEU Plaintiffs' allegations detailing the sophisticated hackings that exposed their deeply personal information—including information that could be used to steal their identities, as in Mr. Gambardella's case—show that NTEU Plaintiffs have sufficiently pled Article III injury under Attias.

2. Attias's ruling on the substantial risk of future harm basis for standing is in line with decisions of the Sixth, Seventh, and Ninth Circuits, and dicta from the Third and Fourth Circuits. These decisions represent the majority view of the courts of appeals on this issue.

The Sixth Circuit has concluded that Article III's injury-in-fact requirement can be satisfied by alleging a substantial risk of future harm where sensitive personal information was taken by a third party who had targeted the information. See Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016). As the Sixth Circuit explained, "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims'

data for the fraudulent purposes alleged in Plaintiffs' complaints." Id.; see id. at 386 (noting hackers stole names, dates of birth, and social security numbers of 1.1 million Nationwide customers).

The Galaria plaintiffs "allege[d] that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of 'possible future injury' or 'objectively reasonable likelihood' of injury that the Supreme Court has explained are insufficient." Id. at 388. "There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals." Id.

The Sixth Circuit's decision embraces Seventh and Ninth Circuit decisions on this issue (Galaria, 663 F. App'x at 389), which are entirely in accord with Attias. See Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015) (concluding that where data breach is perpetrated by a sophisticated thief, it is plausible to assume a substantial risk of harm); Krottner v. Starbucks, Corp., 628 F.3d 1139, 1142-43 (9th Cir. 2010) (standing to sue employer over the theft of personal information because of "anxiety and stress" and increased risk of identity theft). The Ninth Circuit recently reaffirmed its position

that "data breaches in which hackers targeted PII [personally identifiable information] created a risk of harm sufficient to support standing," and it endorsed Attias's reasoning in doing so. In re Zappos.com, Inc., 2018 U.S. App. LEXIS 10031, at *11 n.6 (9th Cir. Apr. 20, 2018).

The Fourth Circuit has expressed a similar view. In a laptop theft case, the court found that plaintiffs did not sufficiently allege standing based on a substantial risk of future harm; but it explicitly noted the absence, in its case, of two types of allegations present in the Sixth, Seventh, and Ninth Circuit decisions cited above: (1) that thieves intentionally targeted the stolen personal information; and (2) that the thieves accessed or misused some of the stolen data. See Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017). If such allegations are made, the Fourth Circuit observed, they "push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." Id. See In re Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 629, 639 n.19 (3d Cir. 2017) (noting the "increased risk of future injury" to plaintiffs "at least weighs in favor of standing" where thief targeted and stole unencrypted personal information that could be

used to perpetrate identity theft and one plaintiff alleged identity theft stemming from the breach).

Other appellate decisions rejecting "substantial risk of future harm" arguments are inapposite. The Eighth Circuit, in In re: SuperValu, Incorporated, Customer Data Security Breach Litigation, 870 F.3d 763 (8th Cir. 2017), left open the question of whether an increased and substantial risk of harm stemming from a data breach, if sufficiently alleged, could qualify as Article III injury. Id. at 769-71 & n.5 (citing Attias). And in the Third Circuit's decision in Reilly v. Ceridian Corporation, there was no indication (unlike in this case) that "the intrusion was intentional or malicious," and "no identifiable taking occurred." 664 F.3d 38, 44 (3d Cir. 2011). Similarly inapt is Whalen v. Michaels Stores, Incorporated, in which the Second Circuit concluded that there was no plausible risk of future harm where plaintiff's credit card information was stolen and the credit card was "promptly canceled after the breach." 689 F. App'x. 89, 90 (2d Cir. 2017) (noting "no other personally identifying information . . . is alleged to have been stolen").

3. The district court ignored the majority appellate view on the "increased risk of future harm" issue and sidestepped Attias,

remarking that "the Court is not persuaded that the holding covers this case." JA425. It concluded that because Attias and out-of-circuit precedent in accord with Attias involved theft of financial information, those decisions were not instructive. JA434-35.

This conclusion ignored the appellate cases, such as Krottner and Galaria, discussed supra, that have found standing based upon a substantial risk of future harm even where it was not financial information that was stolen. The district court's conclusion also ignored that NTEU has pled the theft of financial information. As the district court acknowledged in a footnote, one NTEU Plaintiff specifically alleged that financial information, including investment account information, was provided to OPM, and another NTEU Plaintiff also alleged that financial information was provided to OPM. JA431,n.19.

But, more fundamentally, the district court's analysis is unfaithful to Attias. Although Attias involved the theft of social security numbers and credit card information, its standing analysis was not dependent on, or limited to, those specific types of personal information. Attias specifically held that the allegations of the theft of other, non-financial

data would have been sufficient for standing: "[t]hese portions of the complaint [alleging the theft of other data] would make up, at the very least, a plausible allegation that plaintiffs faced a substantial risk of identity fraud, even if their social security numbers were never exposed to the data thief." 865 F.3d at 628. Attias governs here, and, as discussed above, it confirms NTEU Plaintiffs' standing in this case.

4. The district court's flawed injury-in-fact analysis rested not only on a misinterpretation of appellate precedent—including binding authority—but also assumptions that went far beyond NTEU Plaintiffs' complaint and OPM's arguments for dismissal. It first incorrectly concluded that standing based on a substantial risk of future harm requires the theft of financial information. It then purported to identify of the perpetrator of the OPM data breaches as the Chinese government. JA431-32. And it next speculated, with no basis, as to China's motive in allegedly stealing the personal information involved (something other than financial theft, according to the district court). JA432-33&n.21.

The district court's supposition about China's role in the OPM data breaches and its motivations to justify its standing ruling cannot

withstand scrutiny. First, the district court's conjecture has no support in NTEU Plaintiffs' complaint or even the defendant's arguments; indeed, the government explicitly resisted the district court's invitation to guess the identity of the OPM data breach hacker, let alone that hacker's motivation. JA208-09. Second, the district court's conclusions on these topics appear to conflate NTEU Plaintiffs' allegations with those in superseded complaints in other actions—namely, class action complaints that were superseded by Class Plaintiffs' Consolidated Amended Complaint (CAC). See Gelboim v. Bank of Am. Corp., 135 S. Ct. 897, 904 n.3 (2015). While those superseded complaints "specifically alleged that the breaches were widely reported to have been perpetrated by the Chinese government" (JA431,n.20), NTEU Plaintiffs' complaint did not. JA153-89. The district court cannot use allegations in other complaints as a basis to dismiss NTEU Plaintiffs' action. Third, there is no basis for the district court's speculation that, if China were the hacker, the theft of financial information could not be one of its motives.

5. Finally, while the district court acknowledged, in a footnote, that NTEU Plaintiffs specifically pled that they are at a "substantial

risk of identity theft," it called that allegation "conclusory." JA434,n.22. That label does not hold up, given NTEU Plaintiffs' specific allegations that (1) sophisticated hackers targeted and stole their social security numbers, financial information, and other highly personal information from OPM's databases; (2) this theft puts them at substantial risk of future harm, including identity theft; and (3) illustrating this substantial risk, Plaintiff Gambardella has suffered identity theft that is attributable to the OPM data breaches. JA157-58(¶¶6-8),160-65(¶¶13-32),175-77(¶¶59-66),178(¶¶71-72),180-81(¶¶79-83),181-85(¶¶87-92). Under Attias, these allegations show standing.

b. NTEU Plaintiffs Face A Substantial Likelihood of Having Their Information Stolen Again.

NTEU Plaintiffs have sufficiently alleged a "substantial risk" of "further unauthorized access" of their inherently personal information, and they also allege that any future unauthorized access would again violate their constitutional right to informational privacy. JA181-85(¶¶87-92). Another theft would also amplify the substantial risk of future harm, including identity theft, that already exists for them. JA181-85(¶¶87-92).

NTEU Plaintiffs ground their allegations in reports by OPM's OIG highlighting the continued vulnerability of OPM's databases. JA181-85(¶¶87-91). In its fiscal year 2015 audit report, OPM's OIG reiterated that "the overall lack of compliance that seems to permeate the agency's IT security program" continues, and that it is "very concerned that the agency's systems will not be protected against another attack." JA182(¶88).

On May 18, 2016, the OIG issued another report, stating that it was "even more concerned" about OPM's plans to update its IT security because OPM failed to complete the mandatory planning steps that OMB requires for such a project and failed to develop a "realistic budget" for the effort. JA184(¶91). OPM, moreover, was unable to hire and retain an appropriate contractor to upgrade its IT security. JA183(¶90). OPM hired a vendor with a "troubled history with government contracting" to overhaul its IT infrastructure; on May 9, 2016, that vendor "abruptly ceased operations," with one month left on its contract and the status of its work unknown. JA183(¶90).

The OIG's most recent reports confirm the continued threat to personal information on OPM's databases. In its fiscal year 2017 audit

report, the OIG reported that a "significant" number of OPM information systems continued to lack a valid "Security Assessment and Authorization," meaning that the systems are "at a significantly higher risk of containing unidentified security vulnerabilities."[2] As the OIG explained, if OPM "does not know what weaknesses and vulnerabilities exist in its IT environment, [] it cannot take steps to address and remove those weaknesses." Id. at 6.

Most recently, in a report issued on February 15, 2018, the OIG stated that OPM is "doing it backwards," and trying, in vain, to patch up its antiquated systems, instead of creating a modernized platform that could be adequately secured.[3] As it noted, "[i]t is concerning that almost three years after the data breach of 2015 . . . OPM has still not

---

[2] OPM OIG Office of Audits, Final Audit Report, Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology, i, 6 (June 20, 2017), https://www.opm.gov/our-inspector-general/reports/2017/audit-of-the-us-office-of-personnel-management%E2%80%99s-security-assessment-and-authorization-methodology-4a-ci-00-17-014.pdf.

[3] OPM OIG Office of Audits, Management Advisory, U.S. Office of Personnel Management's Fiscal Year 2017 IT Modernization Expenditure Plan, 2 (Feb. 15, 2018), https://www.opm.gov/our-inspector-general/management-advisory-reports/management-advisory-report-us-office-of-personnel-management%E2%80%99s-fiscal-year-2017-it-modernization-expenditure-plan.pdf.

clearly identified a comprehensive modernization strategy or established the required planning and budgeting mechanisms that would accompany such a project." OPM's response to the report contained no disagreement with it. Id. at Appendix 1-4.

NTEU Plaintiffs' have thus not only pled an Article III injury, but they have also shown their standing to pursue the forward-looking relief sought. Given the continued concerns of OPM's Inspector General, NTEU Plaintiffs are "realistically threatened by a repetition" of the violation of their constitutional rights (Afifi v. Lynch, 101 F. Supp. 3d 90, 109 (D.D.C. 2015)), and have standing to seek declaratory and injunctive relief. See In re Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1220, 1223 (N.D. Cal. 2014) (ruling plaintiffs had standing to seek declaratory and injunctive relief stemming from data breach). Cf. City of Los Angeles v. Lyons, 461 U.S. 95, 109 (1983) (denying injunctive relief for single incident of violence unlikely to reoccur).

B. NTEU Plaintiffs' Injuries Are Fairly Traceable to OPM's Indifference to Securing Their Deeply Personal Information.

1. Each of the Article III injuries that NTEU Plaintiffs allege is "fairly traceable" to OPM. Attias again governs here. There, this Court concluded that plaintiffs' alleged injury (a substantial risk of future

harm) was "fairly traceable" to the breached entity—explicitly rejecting the argument that the alleged injury was "'fairly traceable' only to the data thief." 865 F.3d at 629. Because the Court had to assume for its standing analysis "that plaintiffs will prevail on the merits of their claim that CareFirst failed to properly secure their data and thereby subjected them to a substantial risk of identity theft," it had "little difficulty concluding that their injury in fact is fairly traceable to CareFirst." Id. Accord Galaria, 663 F. App'x at 389 (traceability criterion satisfied because "but for Nationwide's allegedly lax security, the hackers would not have been able to steal Plaintiffs' data").

This reasoning applies here. NTEU Plaintiffs allege that OPM's reckless indifference to its Inspector General's urgent IT security warnings led to data breaches that (1) in and of themselves, violated NTEU Plaintiffs' constitutional right to informational privacy; and (2) put NTEU Plaintiffs at an increased and substantial risk of future harm, including identity theft. JA168-75(¶¶38-58),179(¶¶75-78),181-85(¶¶87-92).

2. The district court side-stepped Attias (again) in its traceability analysis in two ways. First, the district court suggested

Attias's traceability holding was not viable generally because "the issue had not been briefed extensively." JA437. This is a dubious basis for ignoring this Court's precedent. Second, the district court purported to distinguish Attias's traceability ruling because the case involved stolen financial information, which, to the district court, made the Attias plaintiffs' traceability argument stronger. JA437-39. This reasoning is not compelling because none of Attias's conclusions were founded on the theft of financial information, and, in any event, NTEU Plaintiffs pled the theft of financial information. See Section I.A.2.a.3, supra.

The district court also noted that "to hold defendants accountable for plaintiffs' alleged injuries, the Court would have to presume that the vast majority of identity thefts plaintiffs experienced were not perpetrated by other criminals or were not the result of data breaches of other entities." JA439. It added that "[s]uch a presumption, with no factual predicate in the complaints besides allegations based on chronology, stretches the notion of traceability in this case beyond constitutional limits[.]" JA439.

First, the district court's premise is wrong. "That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs

might suffer identity theft or fraud caused by the data stolen in those other breaches . . . is less about standing and more about the merits . . . ." In re Zappos.com, 2018 U.S. App. LEXIS 10031, at *15. Second, the district court's statements cannot be squared with NTEU Plaintiffs' complaint. Plaintiffs Gambardella, Howell, and Ortino each specifically alleged that they had not had their personal information exposed in any other data breach. JA180-81(¶¶82,85-86). The district court, nonetheless, refused to address these allegations. It, instead, referenced them with a "But see" citation in a footnote. JA439,n.27. In other words, the court ignored well-pled allegations that ran counter to its conclusion.

In sum, the district court's traceability ruling conflicts with Attias, ignores critical allegations, and cannot stand.

C. Plaintiffs' Requested Relief Would Remedy Their Injuries.

NTEU Plaintiffs seek a declaration that OPM's failure to protect their personal information was unconstitutional; an order that OPM provide lifetime credit monitoring and identify theft protection to affected NTEU members; an order that OPM correct deficiencies in its IT security; and an order enjoining OPM from collecting additional

personal information from NTEU members electronically until it has taken the necessary steps to safeguard that information. JA186-87.

Declaratory and injunctive relief redress an injury where, as here, the harm to plaintiffs is ongoing. NTEU Plaintiffs continue to face a "substantial risk of further unauthorized access" of their personal information (JA181-84[¶¶87-91]) and a "substantial risk of identity theft" (JA185[¶92]), making their requests for relief appropriate. See, e.g., In re Zappos.com, 2018 U.S. App. LEXIS 10031, at *16 (concluding "requested injunctive relief would limit the extent of the threatened injury by helping Plaintiffs to monitor their credit and the like"); Jewel v. NSA, 673 F.3d 902, 912 (9th Cir. 2011) (standing to seek order enjoining future collection of data); In re Adobe, 66 F. Supp. 3d at 1220 (standing to seek declaratory relief regarding defendant's security measures). See generally Remijas, 794 F.3d at 696-97 (redressability shown because plaintiffs might have future expenses or injuries that favorable ruling would remedy).

II. NTEU Plaintiffs Have Sufficiently Alleged A Breach Of The Constitutional Right To Informational Privacy.

NTEU Plaintiffs have sufficiently alleged their constitutional claim. The constitutionally protected "zone of privacy" involves "at least two different kinds of interests." See Whalen v. Roe, 429 U.S. 589, 598-600 (1977). The pertinent interest here is "the individual interest in avoiding disclosure of personal matters." See id. at 599. Over the last forty years, this right, also known as the constitutional right to informational privacy, has been recognized by the Supreme Court, nearly every court of appeals, and the federal government in litigation.

The right protects individual liberty in two ways, as explained in more detail below. First, it makes the government's power to compel sensitive personal information conditional on the government's ability to show that it will use the compelled information only for legitimate governmental purposes. Second, it makes the government's power to compel sensitive personal information conditional on the government's commitment to keep the information confidential.

The district court's ruling that that constitutional right to informational privacy has no application in the government data breach context (JA453) would eviscerate the right by allowing the government

merely to assert, while doing nothing of substance to demonstrate, a commitment to keep compelled information confidential. It would allow the government to collect inherently personal information from employees based on a commitment of confidentiality and nevertheless do nothing at all to safeguard the information.

The better view of the right, in light of its interpreting jurisprudence, is that the government violates an individual's constitutional right to informational privacy when it compels personal information from the individual based on its commitment to keep the information confidential and then, through reckless indifference to that commitment, facilitates the theft of that information. NTEU Plaintiffs have sufficiently alleged the requisite reckless indifference here (JA185-86[¶¶95-98]), and their Fifth Amendment Due Process Clause claim should be allowed to proceed.

A. The Constitutional Right to Informational Privacy is Firmly Recognized.

The Supreme Court first recognized the constitutional right to informational privacy over forty years ago. In Whalen, the Supreme Court referred to the constitutional privacy "interest in avoiding disclosure of personal matters" while evaluating a state statute

requiring the collection of the names and addresses of all persons prescribed drugs with both legitimate and illegitimate uses. 429 U.S. at 599-600. It concluded that the statute's requirements did not "constitute an invasion of any right or liberty protected by the Fourteenth Amendment." Id. at 600-04. See id. at 606 (Brennan, J., concurring) ("The Court recognizes that an individual's 'interest in avoiding disclosure of personal matters' is an aspect of the right to privacy . . . .").

The unanimous decision in Whalen acknowledged that, while "[t]he concept of a constitutional right of privacy still remains largely undefined," it includes "the right of an individual not to have his private affairs made public by the government." See 429 U.S. at 599-600 & n.24. In the same term as Whalen, the Supreme Court again acknowledged the constitutional right to informational privacy. See Nixon v. Admin. of Gen. Servs., 433 U.S. 425, 457-58 (1977) (discussing the privacy interest described in Whalen while assessing the Presidential Recordings and Materials Preservation Act).

In 2011, the Supreme Court had occasion to revisit this right while analyzing whether parts of standard background investigation

forms violated the right. See NASA v. Nelson, 562 U.S. 134, 159 (2011) ("[W]e conclude that the Government's inquiries do not violate a constitutional right to informational privacy.") (citing Whalen). Although the Court chose to assume, without deciding, that the right existed (562 U.S. at 138), its decision, taken with Whalen and Nixon, show that the Supreme Court has, on three occasions, analyzed claims based on the constitutional right to informational privacy. Two other Supreme Court opinions, moreover, "have mentioned the concept in passing and in other contexts." See id. at 146 (citing Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989) and New York v. Ferber, 458 U.S. 747 (1982)).

Nearly every federal court of appeals has taken the Supreme Court's cue and recognized the right. After Whalen and Nixon issued, the Second, Third, Fourth, Fifth, Seventh, Eighth, Ninth, Tenth, and Eleventh Circuits recognized the constitutional right to privacy in the nondisclosure of personal information.[4] The Sixth Circuit has left open

[4] See, e.g., Denius v. Dunlap, 209 F.3d 944, 955-56 (7th Cir. 2000); Ferm v. United States, 194 F.3d 954, 958-60 (9th Cir. 1999); Eagle v. Morgan, 88 F.3d 620, 625 (8th Cir. 1996); Sheets v. Salt Lake Cnty., 45 F.3d 1383, 1388 (10th Cir. 1995); James v. Douglas, 941 F.2d 1539, 1544 (11th Cir. 1991); Woodland v. City of Houston, 940 F.2d 134, 138

the question of the right's existence. See J.P. v. DeSanti, 653 F.2d 1080, 1090-91 (6th Cir. 1981).

The D.C. Circuit has not had occasion to rule squarely on the right's existence. Several panels of the Court have indicated, in dicta, that the right exists. See, e.g., United States v. Hubbard, 650 F.2d 293, 304-05 & nn.38-39 (D.C. Cir. 1980) (citing Whalen with approval and concluding that the Fifth Amendment's "protection of liberty from federal intrusion . . . can be no less comprehensive" than the Fourteenth Amendment's "sphere of personal liberty"); Doe v. Webster, 606 F.2d 1226, 1238 n.49 (D.C. Cir. 1979) ("The right to privacy . . . 'should encompass a substantial measure of freedom for the individual to choose the extent to which the government could divulge criminal information about him, at least where no conviction has ensued and no countervailing government interest is demonstrated.'") (internal quotation omitted); see also Nat'l Fed'n of Fed. Emps. v. Greenberg, 983 F.2d 286, 295-96 (D.C. Cir. 1993) (Edwards, J., concurring) ("I find no

(5th Cir. 1991); Walls v. Petersburg, 895 F.2d 188, 192-95 (4th Cir. 1990); Barry v. City of New York, 712 F.2d 1554, 1558-64 (2d Cir. 1983)); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577-80 (3d Cir. 1980).

'ambiguity' in the core principle undergirding the Supreme Court's decision in Whalen . . . .").

One panel of the Court, in dicta, expressed "doubts" as to the right's existence. AFGE v. HUD, 118 F.3d 786, 791-92 (D.C. Cir. 1997). Two members of another panel suggested that they found "ambiguity" in Whalen's ruling. Greenberg, 983 F.2d at 293-94.

Consistent with the majority view, the federal government has acknowledged the right's existence in litigation. In Nelson, the government outlined to the Supreme Court what it believes to be the scope and application of the "Whalen And Nixon Framework."[5] It flatly stated that Whalen and Nixon "defined protection against public disclosure as the core of the informational privacy right." Reply Brief for the Petitioners, NASA v. Nelson, 2010 U.S. S. Ct. Briefs LEXIS 1494, at *5 (Sept. 1, 2010). And it rejected the notion "that the informational privacy right 'protects only against public dissemination of private information.'" Id. at *8.

[5] See Brief for the Petitioners, NASA v. Nelson, 2010 U.S. S. Ct. Briefs LEXIS 448, at *37-46, *69-72, *78-92 (May 20, 2010).

It should thus be beyond dispute that the right exists, leaving only its contours to be determined. Those contours should be determined in a manner consistent with the right's nature and purpose, as discussed below.

B. The Right Requires the Government to Protect Personal Information Entrusted to it.

Once recognizing that the constitutional right to informational privacy protects inherently personal information from disclosure to the government, four courts of appeals have concluded that, when individuals provide such information to the government based on a promise of confidentiality, the right is violated if the government disregards that promise and allows unauthorized access to that information. It must follow that the right may serve as the basis for a claim where the government ignores its obligation to secure constitutionally-protected information that it collected on a promise of confidentiality. JA162-65(¶¶20-31),168-75(¶¶38-58),177-78(¶¶66-70),185-86(¶¶96-98).

1. In Fadjo v. Coon, for example, the Fifth Circuit recognized the right discussed in Whalen and ruled that the plaintiff sufficiently alleged a claim based on the right. See 633 F.2d 1172, 1175 (5th Cir.

1981). In Fadjo, the state subpoenaed testimony from the plaintiff concerning "the most private details of his life," which the plaintiff provided on the assurances that his testimony was "absolutely privileged" under state law and that the "contents of his testimony would be revealed to no one." Id. at 1174. The state then disclosed that information to various third parties. Id.

The Fifth Circuit noted that "the right to privacy consists of two interrelated strands: 'One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.'" Id. at 1175 (quoting Whalen, 429 U.S. at 599-600). "Both strands may be understood as aspects of the protection which the privacy right affords to individual autonomy and identity. . . . The first strand, however, described by this circuit as 'the right to confidentiality,' . . . is broader in some respects." Id.

The court concluded that the plaintiff's claim was based upon the "right to confidentiality." Id. It took as true his allegation that the information concerned "the most private details of his life." Id. at 1174. It then concluded that his claim was adequately pled because "the state

may have invaded [plaintiff's] privacy in revealing it to [third parties]." Id. at 1175. Accord James v. Douglas, 941 F.2d 1539, 1543-44 & n.8 (11th Cir. 1991) (embracing Fadjo and ruling that complaint sufficiently alleged a violation of a "clearly established constitutional right" where it alleged that police allowed unauthorized individuals to view plaintiff's sex tape seized as evidence).

In Eagle v. Morgan, the Eighth Circuit demonstrated a similar understanding of the constitutional right to informational privacy. In Eagle, law enforcement officials disclosed an individual's prior guilty plea at a city council meeting. 88 F.3d 620, 624-25 (8th Cir. 1996). The individual sued, alleging, among other claims, breach of his constitutional right to privacy. Id. The Eighth Circuit entertained his claim, noting its view that "[t]his protection against public dissemination of information is limited and extends only to highly personal matters representing 'the most intimate aspects of human affairs.'" Id. at 625.

In the court's view, to violate the constitutional right (1) the information disclosed must be inherently intimate information of the type historically protected in constitutional jurisprudence, such as

information about one's spouse obtained through marriage, medical information, and certain financial information; and (2) the disclosure "'must be either a shocking degradation or an egregious humiliation of her to further some specific state interest, or a flagrant bre[a]ch of a pledge of confidentiality which was instrumental in obtaining the personal information.'" Id.

The court thus proceeded to "examine the nature of the material opened to public view to assess whether the person had a legitimate expectation that the information would remain confidential while in the state's possession." Id. It concluded that the plaintiff failed to state a claim because the prior guilty plea was made in open court and thus was public information. Id. at 625-26.

The Tenth Circuit's decision in Sheets v. Salt Lake County used a similar analysis. In Sheets, the plaintiff turned over the private diary of his murdered wife to police investigating her murder. 45 F.3d 1383, 1386 (10th Cir. 1995). One of the investigating detectives told him that "the diary would remain confidential." Id. Copies of the diary were distributed to officers on the case, one of whom allegedly shared photocopies of, and notes about, the diary with an author. Id. That

author published a book about the murder with direct quotations from the diary. Id.

The Tenth Circuit, endorsing Whalen's views on the constitutional right to informational privacy, explained that "'due process . . . implies an assurance of confidentiality with respect to certain forms of personal information possessed by the state.'" Id. at 1387. It then discussed the factors used to assess whether right was violated. Id. It explained that (1) "[i]nformation falls within the ambit of constitutional protection when an individual has a 'legitimate expectation . . . that it will remain confidential while in the state's possession'"; and (2) the "legitimacy of this expectation depends, 'at least in part, upon the intimate or otherwise personal nature of the material which the state possesses.'" Id.

Using this framework, the Tenth Circuit ruled that the information—plaintiff's wife's "written perceptions of their marriage"—was protected by the constitutional right and that "there was ample evidence for a jury to conclude that [plaintiff] legitimately expected his wife's diary to remain confidential while in the hands of the police." Id.

at 1388-89 (affirming district court's denial of defendant's motion for judgment as a matter of law).

2. These appellate decisions—though they come in the context of the government affirmatively providing the protected information to those unauthorized to view it—show that four circuits, once recognizing the right, have imputed to the government an affirmative obligation not to disclose material protected by the right that it promised to keep confidential. If this affirmative obligation is violated when the government intentionally discloses such information, it must follow that the right is also violated when the government effectively leaves that information in a room with all the doors and windows open. A contrary view would be incompatible with the core purpose of the right: protecting the confidentiality of fundamentally personal information.

These decisions, relegated to a footnote by the district court (JA453,n.30), thus show that OPM had (and still has) an affirmative duty, rooted in the constitutional right to informational privacy itself, to protect the inherently personal data entrusted to it. This affirmative duty is consistent with substantive due process principles. As one scholar has explained,

> [w]hen the State takes a person's data and holds it in a fashion outside the person's control, the State has done to that data exactly what Chief Justice Rehnquist said was necessary to trigger Due Process Clause protection: it has 'by the affirmative exercise of its power' taken the data and 'so restrain[ed]' it that the original owner is unable to exert any control whatsoever over how the government stores or secures it. The government's 'affirmative duty to protect' the data 'arises . . . from the limitation which it has imposed on his freedom to act on his own behalf' to keep the data secure.

A. Michael Froomkin, Government Data Breaches, 24 Berkley Tech. L. J. 1019, 1049 (2009) (addressing DeShaney v. Winnebago Cnty. Dep't of Soc. Servs., 489 U.S. 189 (1989)).

Here, OPM took possession of the intimate personal information of NTEU members—which it required to be provided as a condition of employment—and explicitly promised that it would keep the information confidential. JA162-65(¶¶20-31),176-78(¶¶60-70),185(¶96). OPM alone determined how to protect that information, rendering the "original owners" of the information, NTEU's members, powerless in terms of securing it. See Froomkin, 24 Berkley Tech. L. J. at 1049. OPM's conscious and extended failure to secure its information systems are analogous to the government actions in the courts of appeals cases discussed above. Those cases show that OPM breached its affirmative

duty to keep inherently personal information confidential (JA185-86[¶¶96-98]).

Though grounded in this authority, the district court resisted the basis of NTEU Plaintiffs' claim. In its view, "[a]t bottom, what NTEU [P]laintiffs allege is a violation of the Privacy Act." JA454. The Privacy Act does not supplant the constitutional right to informational privacy. Whalen anticipated a claim like the one raised here. It explicitly left open the possibility that an "unwarranted disclosure of accumulated private data – whether intentional or unintentional – or by a system that did not contain [adequate] security provisions" could be held to violate the constitutional right to informational privacy, notwithstanding any "concomitant statutory or regulatory duty to avoid unwarranted disclosures." See 429 U.S. at 605-06. Moreover, the types of common-sense relief that NTEU Plaintiffs request are not available under the Privacy Act.

In sum, four courts of appeals have used the analysis described above to assess claims based on a constitutional right to informational privacy that arise after a disclosure has been made to the government.

As shown below, using this framework, NTEU Plaintiffs have sufficiently alleged their claim.

C. NTEU Plaintiffs Sufficiently Allege That OPM's Databases House Their Constitutionally Protected Information.

There is no complete catalog of the types of personal information that are protected by the constitutional right to informational privacy. See Fraternal Order of Police, Lodge 5 v. City of Philadelphia, 812 F.2d 105, 116 (3d Cir. 1987) ("When the information is inherently private, it is entitled to protection."). Courts have held that, at a minimum, the following types of personal information are protected by the right:

1. Information about one's spouse acquired through marriage;[6]
2. Financial information;[7]
3. Medical information;[8] and

[6] See Sheets, 45 F.3d at 1387-89 (discussing "information conveyed to one's spouse or that one's spouse has observed about one's character, marriage, finances, and business"); Eagle, 88 F.3d at 625.

[7] See Fraternal Order of Police, 812 F.2d at 115; Barry, 712 F.2d at 1559.

[8] See Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260, 1269 (9th Cir. 1998).

4. Social security numbers.[9]

Plaintiffs Gambardella, Howell, and Ortino were among the NTEU members who provided precisely these types of intimate personal information to OPM, which, in turn, stored it on its databases. JA177(¶66). They, like other NTEU members, provided OPM with completed standard background investigation forms that required them to provide among other things, medical information (including mental health information), marital information, and social security numbers. JA162-65(¶¶20-31),177(¶66). These documents also require an "Authorization for Release of Information" that allows background investigators to obtain "any information" relating to the individual's "activities" from any individual, employer, credit bureau, retail business establishment, or any "other sources of information." JA163-65(¶¶22,25,30).

NTEU Plaintiffs have thus sufficiently alleged that every NTEU member who provided personal information to OPM—whether that information was a social security number or the full array of

[9] See Ferm, 194 F.3d at 958-60; Arakawa v. Sakata, 133 F. Supp. 2d 1223, 1228-29 (D. Haw. 2001).

information in a standard background investigation file—gave OPM constitutionally-protected information.

D. NTEU Plaintiffs Sufficiently Allege that OPM's Failure to Safeguard the Protected Information, Leading to Its Taking, Violated the Right.

The complaint alleges that OPM breached its explicit promise to keep NTEU members' inherently private information—including information of the type that the Constitution historically protects (JA162-65[¶¶20-31])—confidential. JA168-75(¶¶38-58);177-78(¶¶66-70),185-86(¶¶96-98). It describes, in detail, OPM's failure to follow its Inspector General's urgent recommendations for nearly a decade, creating an environment in which the information provided by NTEU members was vulnerable to the type of thefts that OPM announced in June 2015. JA168-75(¶¶38-58). Those allegations are sufficient to state a claim. See Fadjo, 633 F.2d at 1175 (assessing whether personal information at issue was protected by the right and whether there was a breach of a promise of confidentiality used to obtain that information); James, 941 F.2d at 1544 (same); Sheets, 45 F.3d at 1387 (same); Eagle, 88 F.3d at 625 (same).

For years leading up to the breaches announced in June 2015, OPM's OIG alerted OPM to several serious deficiencies in its information technology security programs and practices. JA168-75(¶¶38-58). OPM's Inspector General testified that OPM's failure to update its cybersecurity "without question . . . exacerbated the possibility" of a breach. JA174-75(¶56). See JA175(¶57) ("We're a wonderful poster child of how bad it can be if you don't do the right thing," remarked Clifton Triplett, OPM's senior cybersecurity advisor).

Despite these known and sustained deficiencies, OPM promised current and prospective federal employees who were required to submit inherently personal information to it that it would "protect [the data] from unauthorized disclosure." JA177-78(¶¶67-70). NTEU Plaintiffs' allegations concerning OPM's reckless and continued indifference to safeguarding the types of information protected by the constitutional right to informational privacy—information that it promised to keep confidential (JA177-78[¶¶66-70])—thus state a plausible claim for relief. JA185-86(¶¶92-98). Drawing all reasonable inferences in NTEU Plaintiffs' favor and accepting their allegations as true, their complaint sufficiently states a claim against OPM.

CONCLUSION

For the foregoing reasons, NTEU Plaintiffs respectfully request that this Court reverse the district court's rulings that NTEU Plaintiffs lack standing and, alternatively, that they failed to state a claim.

Respectfully submitted,

/s/ Gregory O'Duden
GREGORY O'DUDEN
General Counsel

/s/ Larry J. Adkins
LARRY J. ADKINS
Deputy General Counsel

/s/ Paras N. Shah
PARAS N. SHAH
Assistant Counsel

/s/ Allison C. Giles
ALLISON C. GILES
Assistant Counsel

NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
Tel: (202) 572-5500
Email: greg.oduden@nteu.org
Email: larry.adkins@nteu.org
Email: paras.shah@nteu.org
Email: allie.giles@nteu.org

Counsel for NTEU Plaintiffs

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations set forth in Circuit Rule 32 because it contains 9744 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

This brief likewise complies with this Court's order dated March 26, 2018, which allows appellants in this consolidated action a total of 22,000 words for their respective opening briefs, to be divided as appellants see fit. Counsel for appellants conferred and agreed that appellants in Case No. 17-5217 would use no more than 10,000 words for their opening brief, while appellants in Case No. 17-5232 would use no more than 12,000 words for theirs.

This brief also complies with the typeface and type style requirements of Federal Rule of Appellate Procedure 32(a)(5) and (6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in fourteen-point Century font.

/s/ Paras N. Shah

PARAS N. SHAH
Assistant Counsel

NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
(202) 572-5500
paras.shah@nteu.org

Counsel for Appellants
National Treasury Employees Union,
Eugene Gambardella,
Stephen Howell, and
Jonathon Ortino

May 10, 2018

CERTIFICATE OF SERVICE

I certify that, on May 10, 2018, I electronically filed the foregoing document with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit through the appellate CM/ECF system. I further certify that the foregoing document is being served on all counsel of record via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ Paras N. Shah

PARAS N. SHAH
Assistant Counsel

NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
(202) 572-5500
paras.shah@nteu.org

Counsel for Appellants
National Treasury Employees Union,
Eugene Gambardella,
Stephen Howell, and
Jonathon Ortino

May 10, 2018

ADDENDUM

RELEVANT STATUTORY PROVISIONS

Pursuant to Federal Rule of Appellate Procedure 28(f) and Circuit Rule 28(a)(5), the following statutes are included in this Addendum:

	Page No.
28 U.S.C. § 1291	A3
28 U.S.C. § 1331	A3
44 U.S.C. § 3554	A4

28 U.S.C. § 1291. Final decisions of district courts.

The courts of appeals (other than the United States Court of Appeals for the Federal Circuit) shall have jurisdiction of appeals from all final decisions of the district courts of the United States, the United States District Court for the District of the Canal Zone, the District Court of Guam, and the District Court of the Virgin Islands, except where a direct review may be had in the Supreme Court. The jurisdiction of the United States Court of Appeals for the Federal Circuit shall be limited to the jurisdiction described in sections 1292(c) and (d) and 1295 of this title [28 USCS §§ 1292(c) and (d) and 1295].

28 U.S.C. § 1331. Federal question.

The district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.

44 U.S.C. § 3554. Federal agency responsibilities.

(a) In general. The head of each agency shall--

(1) be responsible for--

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of--

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter [44 USCS §§ 3551 et seq.] and related policies, procedures, standards, and guidelines, including--

(i) information security standards promulgated under section 11331 of title 40 [40 USCS § 11331];

(ii) operational directives developed by the Secretary under section 3553(b) [44 USCS § 3553(b)];

(iii) policies and procedures issued by the Director;

(iv) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

(v) emergency directives issued by the Secretary under section 3553(h) [44 USCS § 3553(h)]; and

(C) ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes;

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through--

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40 [40 USCS § 11331], for information security classifications and related requirements;
(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and
(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) delegate to the agency Chief Information Officer established under section 3506 [44 USCS § 3506] (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter [44 USCS §§ 3551 et seq.], including--
(A) designating a senior agency information security officer who shall--
(i) carry out the Chief Information Officer's responsibilities under this section;
(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;
(iii) have information security duties as that official's primary duty; and
(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;
(B) developing and maintaining an agencywide information security program as required by subsection (b);
(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title [44 USCS § 3553] and section 11331 of title 40 [40 USCS § 11331];
(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter [44 USCS §§ 3551 et seq.] and related policies, procedures, standards, and guidelines;

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;

(6) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter [44 USCS §§ 3551 et seq.] as directed by the official delegated authority under paragraph (3); and

(7) ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

(b) Agency program. Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes--

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40 [40 USCS § 11331];

(2) policies and procedures that--

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level;
(C) ensure that information security is addressed throughout the life cycle of each agency information system; and
(D) ensure compliance with--
(i) the requirements of this subchapter [44 USCS §§ 3551 et seq.];
(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40 [40 USCS § 11331];
(iii) minimally acceptable system configuration requirements, as determined by the agency; and
(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of--
(A) information security risks associated with their activities; and
(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing--
(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c) [44 USCS § 3505(c)];
(B) may include testing relied on in an evaluation under section 3555 [44 USCS § 3555]; and

(C) shall include using automated tools, consistent with standards and guidelines promulgated under section 11331 of title 40 [40 USCS § 11331];

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, which--

(A) shall be consistent with the standards and guidelines described in section 3556(b) [44 USCS § 3556(b)];

(B) may include using automated tools; and

(C) shall include--

(i) mitigating risks associated with such incidents before substantial damage is done;

(ii) notifying and consulting with the Federal information security incident center established in section 3556 [44 USCS § 3556]; and

(iii) notifying and consulting with, as appropriate--

(I) law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel;

(II) an office designated by the President for any incident involving a national security system;

(III) for a major incident, the committees of Congress described in subsection (c)(1)--

(aa) not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and

(bb) after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and

(IV) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) Agency reporting.

(1) Annual report.

(A) In general. Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including--

(i) a description of each major information security incident or related sets of incidents, including summaries of--

(I) the threats and threat actors, vulnerabilities, and impacts relating to the incident;

(II) the risk assessments conducted under section 3554(a)(2)(A) [44 USCS § 3554(a)(2)(A)] of the affected information systems before the date on which the incident occurred;

(III) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and

(IV) the detection, response, and remediation actions;

(ii) the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

(iii) a description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director, including--

(I) the number of individuals whose information was affected by the major information security incident; and

(II) a description of the information that was breached or exposed; and

(iv) any other information as the Director or the Secretary, in consultation with the Director, may require.

(B) Unclassified report.

(i) In general. Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

(ii) Access to information. The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

(2) Other plans and reports. Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

(d) Performance plan.

(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 [31 USCS § 1115] a description of--

(A) the time periods; and

(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(1).

(e) Public notice and comment. Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.