67 FLRA No. 126

UNITED STATES
DEPARTMENT OF HOMELAND SECURITY
U.S. IMMIGRATION
AND CUSTOMS ENFORCEMENT
(Agency)

and

AMERICAN FEDERATION
OF GOVERNMENT EMPLOYEES
NATIONAL IMMIGRATION
AND CUSTOMS ENFORCEMENT
COUNCIL 118
(Union)

0-AR-4946

_____

DECISION

July 8, 2014

_____

Before the Authority: Carol Waller Pope, Chairman, and Ernest DuBester and Patrick Pizzella, Members
(Member Pizzella dissenting)

I. Statement of the Case

The Union filed a grievance alleging that the Agency blocked access to commercial, web-based email services (webmail) on the Agency's network without first satisfying its bargaining obligations to the Union. Arbitrator Jeffrey J. Goodfriend sustained the grievance, and, as a remedy, he directed the Agency to bargain with the Union. In an exception to the award, the Agency contends that certain provisions of the Federal Information Security Management Act (FISMA)[1] grant the Agency sole and exclusive discretion to determine its network-access policies – in other words, the right to determine those policies without bargaining at all with the Union – and, thus, that the Arbitrator's direction to bargain over such matters is contrary to law. Because the plain wording and legislative history of the cited provisions do not support the Agency's claim of sole and exclusive discretion, we deny the Agency's exception.

[1] 44 U.S.C. §§ 3541-3549.

II. Background and Arbitrator's Award

Following months of discussion among Agency managers about whether to block webmail access on the Agency's network, the Agency notified the Union that it had decided to terminate employees' webmail access, effective one week after the notice. When the Agency instituted the webmail block without bargaining, the Union filed a grievance. The grievance went to arbitration, where the Arbitrator framed the issues to include whether: (1) the Agency was "entitled to 'expedited implementation'" of webmail-access changes under the parties' agreement;[2] (2) FISMA "place[d] [i]nformation[-]system configurations under the 'sole and exclusive discretion' of [Agency m]anagement"; and (3) the Agency improperly "block[ed] webmail."[3]

Before the Arbitrator, the Agency asserted that the parties' agreement authorized blocking webmail without pre-implementation bargaining because the agreement recognized the "need" on "certain occasions . . . for expedited implementation of new policies or practices affecting conditions of employment."[4] In particular, the Agency asserted that the urgency of webmail-security threats required that it act without bargaining first. But the Arbitrator rejected that contention, due to: (1) the Agency's having permitted "open and frequent" violations of its webmail policy for more than two years before the grievance;[5] (2) the six-month delay between management's decision to block webmail and the implementation of that block; and (3) the Agency's decision to un-block webmail for two months in response to a complaint from another Department of Homeland Security component. The Arbitrator found that the "Agency's less than deliberate and speedy attention to this matter" belied any claim that "'expedited implementation' was . . . necessary" here.[6]

The Agency also contended before the Arbitrator that it possessed sole and exclusive discretion to configure its information systems – including their access policies – because FISMA required the Agency to "provide information security" for the "information systems . . . under [its] control, including through implementing policies and procedures to cost-effectively reduce risks to an acceptable level."[7] In addition, the

[2] Award at 19.
[3] *Id.* at 18.
[4] *Id.* at 38 (quoting Collective-Bargaining Agreement (CBA), Art. 9(F)).
[5] *Id.* at 39.
[6] *Id.*
[7] *Id.* at 28 (quoting 44 U.S.C. § 3544(a)(2)(C)) (internal quotation marks omitted) (mistakenly identified in award as § 3555(a)(2)); *accord* Exceptions, Attach., Agency's Post-Hr'g Br. to Arbitrator (Post-Hr'g Br.) at 62 (quoting 44 U.S.C. § 3544(a)(2)(C)).

Agency argued that its obligation under FISMA to "ensure compliance with . . . minimally acceptable system[-]configuration requirements, as determined by the [A]gency," required finding that the Agency had sole and exclusive discretion over such matters.[8] While conceding that the text of "FISMA does not expressly provide for such discretion," the Agency argued that its FISMA responsibilities "'strongly suggest[]' that [network-]access issues are within the 'sole and exclusive discretion' of the Agency."[9] But the Arbitrator rejected those arguments and found that "nothing in the FISMA statute . . . provides for such discretion."[10]

The Arbitrator found that the Agency violated its bargaining obligations in instituting the webmail block, but he did not direct the Agency to restore employees' access to webmail. Instead, he directed the Agency to bargain over the impact and implementation of the change in webmail access.

The Agency filed an exception to the award, and the Union filed an opposition to the Agency's exception.

III. Preliminary Matter: Sections 2425.4(c) and 2429.5 of the Authority's Regulations bar some of the Agency's arguments.

Under §§ 2425.4(c) and 2429.5 of the Authority's Regulations, the Authority will not consider any arguments that could have been, but were not, presented to the arbitrator.[11] To support its claim of sole and exclusive discretion before the Arbitrator, the Agency relied on two provisions of FISMA that are also raised in the Agency's exception – 44 U.S.C. § 3544(a)(2)(C) and (b)(2)(D)(iii). But in its exception, the Agency also relies on several statutory provisions and an executive order that it did not raise below – specifically, 5 U.S.C. §§ 7103(a)(3)(b), (c), (d), and (h),[12] 7103(b)(1)(A),[13] 7106(a)(2)(D),[14] and 7112(b)(6);[15] 44 U.S.C. §§ 3524 (which does not exist),[16] 3536,[17] and 3542(b)(2)(A);[18] and Executive Order 13,480.[19] Because the Agency could have, but did not, raise these other authorities before the Arbitrator, §§ 2425.4(c) and 2429.5 bar the Agency from relying on them in its exception to the award. Therefore, we decline to consider the Agency's arguments regarding the statutory provisions and executive order that were not raised before the Arbitrator. As such, we address only the argument that the Agency presented to the Arbitrator – specifically, that § 3544(a)(2)(C) and (b)(2)(D)(iii) of FISMA grants the Agency sole and exclusive discretion.

IV. Analysis and Conclusion: The award is not contrary to law.

The Agency argues that the Authority should interpret FISMA as giving the Agency sole and exclusive discretion to take "security actions to protect" information systems under the Agency's control,[20] and the Agency contends that the webmail block in this case was such an action. Matters concerning conditions of employment over which an agency has discretion are negotiable if the agency's discretion is not sole and exclusive, and if the matters to be negotiated are not otherwise inconsistent with law or applicable rule or regulation.[21] In resolving claims of sole and exclusive discretion, the Authority "examines the plain wording and the legislative history of the statute being relied on."[22] For example, the Authority has found sole and exclusive discretion where a statute empowered an agency to act "without regard to the provisions of other laws applicable to officers or employees of the United States,"[23] and also when a statute provided that an agency's conduct "shall not be limited by . . . any provision of law . . . relating to the methods of involving . . . labor organizations . . . in personnel decisions."[24] Although a law need "not use any specific phrase or

[8] Award at 28 (quoting 44 U.S.C. § 3544(b)(2)(D)(iii)) (omission in award) (internal quotation marks omitted); *accord* Post-Hr'g Br. at 62 (quoting 44 U.S.C. § 3544(b)(2)(D)(iii)).
[9] Award at 28 (quoting Post-Hr'g Br. at 62).
[10] *Id.*
[11] 5 C.F.R. §§ 2425.4(c), 2429.5.
[12] Exception at 9.
[13] *Id.* at 8.
[14] *Id.* at 6.
[15] *Id.* at 8-9.
[16] *Id.* at 6.
[17] *Id.* at 5, 6.
[18] *Id.* at 4.
[19] *See id.* at 8.
[20] *Id.* at 3.
[21] *E.g., Dep't of VA, VA Med. Ctr., Veterans Canteen Serv., Lexington, Ky.*, 44 FLRA 162, 164 (1992) (*VAMC*) (citing *U.S. DOD, Office of Dependents Sch.*, 40 FLRA 425, 441-43 (1991); *NTEU*, 30 FLRA 677, 682 (1987) (where statute authorized the head of the agency "to establish or provide for the establishment of appropriate fees and charges," the Authority found that the "statute leaves the [a]gency with discretion to determine the appropriate fees")).
[22] *NAGE, Local R5-136*, 56 FLRA 346, 348 (2000) (quoting *Ass'n of Civilian Technicians, Mile High Chapter*, 53 FLRA 1408, 1412 (1998)) (internal quotation marks omitted).
[23] *AFGE, Local 3295*, 47 FLRA 884, 894 (1993) (Member Talkin dissenting) (quoting 12 U.S.C. § 1462a(g) (1993)), *aff'd*, 46 F.3d 73 (D.C. Cir. 1995); *see id.* at 894-99 (analyzing claim of sole and exclusive discretion).
[24] *U.S. Dep't of the Interior, Bureau of Indian Affairs, Sw. Indian Polytechnic Inst., Albuquerque, N.M.*, 58 FLRA 246, 248-49 (2002) (third and fourth omissions in original) (quoting Haskell Indian Nations University and Southwestern Indian Polytechnic Institute Administrative Systems Act of 1998, § 4(a), 25 U.S.C. § 3731 note); *see id.* at 248-50 (analyzing claim of sole and exclusive discretion).

words in order to confer sole and exclusive discretion,"[25] the absence of wording that expressly preempts the Federal Service Labor-Management Relations Statute or other laws is a "strong indication that Congress did not intend the [agency] to have unfettered discretion"[26] over a matter.

The Agency contends that its obligation under § 3544 of FISMA to "provide information security for the information and information systems . . . under [its] control"[27] indicates a congressional desire "to let the Agency act with absolute discretion" in matters of information security.[28] (Although the exception quotes 44 U.S.C. § 3534 for support,[29] 44 U.S.C. § 3549 provides that § 3544 supersedes § 3534,[30] so we have considered § 3544 in our analysis.) But as the Agency conceded before the Arbitrator, § 3544 does not "expressly provide for such discretion."[31] That absence of preemptive wording is a "strong indication that Congress did not intend the [Agency] to have unfettered discretion" in matters of information security.[32] Further, the text of § 3544 is not similar to any statutory wording that the Authority or the courts have previously recognized as conferring sole and exclusive discretion.[33]

With regard to FISMA's legislative history, the Agency argues that the Authority should interpret FISMA in light of Congress's concern with "terrorists, transnational criminals, and foreign intelligence services . . . us[ing] tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to information and systems."[34] The Agency also contends that, because "the level of protection that agencies provide should be commensurate with the risk to agency operations and assets,"[35] the protection of information systems containing criminal-investigative materials should be under an agency's sole and exclusive discretion. However, neither Congress's concern with the security of information systems, nor its conviction that agencies should tailor their responses to address that concern, demonstrates congressional intent to vest the Agency with sole and exclusive discretion over information-security matters. In other words, the legislative history is consistent with the Agency's obligation to bargain to the extent of its discretion regarding its information-security policies.

The dissent disagrees with our analysis, but does not explain how the wording or the legislative history of 44 U.S.C. § 3544(a)(2)(C) and (b)(2)(D)(iii) supports the Agency's claim of sole and exclusive discretion. Rather, the dissent focuses on the number of pages in the arbitration-hearing transcript and the Agency's brief;[36] a vacated federal-district-court opinion;[37] the appeals-court decision that vacated that district-court opinion (and that, as the appeals court stated, did not involve "FISMA compliance");[38] and the number of cyber attacks at agencies other than the one in this dispute.[39] Those factors provide no basis for finding sole and exclusive discretion. And although the dissent quotes extensively from post-enactment FISMA guidance[40] – which, by definition, is not FISMA's legislative history – none of that guidance indicates congressional intent to preempt the Statute either. Further, the dissent's suggestion that the Statute should not apply in this case because Congress enacted it before the "advent of the internet,"[41] is unsupported. Indeed, courts employ the very opposite presumption: "[S]tatutes continue in force until abrogated by subsequent action of the legislature."[42] In this respect, we agree with the U.S. Court of Appeals for the Second Circuit, which explained that "we cannot simply say [a] statute is 'too old' and decline to apply it to . . . newer technology."[43] And besides that general presumption, we note that one of the Statute's primary architects specifically stated that the Authority should

[25] *Id.* at 248 (citing *Ass'n of Civilian Technicians, Tex. Lone Star Chapter 100*, 55 FLRA 1226, 1229 n.7 (2000)).
[26] *VAMC*, 44 FLRA at 165.
[27] Exception at 5 n.2 (quoting 44 U.S.C. § 3534).
[28] *Id.* at 6.
[29] *Id.* at 5 n.2 (quoting 44 U.S.C. § 3534).
[30] *See* 44 U.S.C. § 3549 ("While this subchapter [44 U.S.C. §§ 3541-49] is in effect, subchapter II of this chapter [44 U.S.C. §§ 3531-38] shall not apply.").
[31] Award at 28.
[32] *VAMC*, 44 FLRA at 165.
[33] *See id.* at 164-65 (statutory provision stating that the "Secretary shall . . . fix the prices of merchandise and services in canteens" did not prohibit agency from setting prices through negotiation; provision simply granted Secretary discretion to fix prices (quoting 38 U.S.C. § 7802)); *cf., e.g.*, *NTEU v. FLRA*, 435 F.3d 1049, 1051-53 (9th Cir. 2006) (provision giving Comptroller of the Currency authority to employ and compensate employees "without regard to the provisions of other laws applicable to officers or employees of the United States" granted sole and exclusive discretion (quoting 12 U.S.C. § 481) (emphasis omitted)).
[34] Exception at 3 (quoting H.R. Rep. No. 107-787, pt. 1, at 55 (2002)) (internal quotation mark omitted).
[35] *Id.* at 4 (quoting H.R. Rep. No. 107-787, pt. 1, at 57) (internal quotation mark omitted).
[36] Dissent at 11.
[37] *E.g.*, *id.* at 9 & nn.5-6 (citing *Cobell v. Norton*, 394 F. Supp. 2d 164, 173 (D.D.C. 2005), *vacated*, *Cobell v. Kempthorne*, 455 F.3d 301, 317 (D.C. Cir. 2006) (*Kempthorne*)).
[38] *Kempthorne*, 455 F.3d at 314.
[39] Dissent at 10.
[40] *E.g.*, *id.* at 9 nn.2 & 4; *id.* at 10 n.15; *id.* at 12 n.36; *id.* at 13 nn.44 & 46.
[41] *Id.* at 10.
[42] 2 Norman J. Singer & J.D. Shambie Singer, *Sutherland Statutory Construction* § 34:1, at 32 (7th ed., 2009 new ed.).
[43] *IRS v. Worldcom, Inc.*, 723 F.3d 346, 364 (2d Cir. 2013).

treat the "concept of negotiability" as a "dynamic and growing one" such that it would never presume, as the dissent does, that the Statute was insufficiently "responsive to changing and particularized circumstances."[44]

As for the dissent's suggestion that FISMA should be read to confer sole and exclusive discretion because it deals with time-sensitive information-security threats, there is no dispute that Congress considered an agency's right to safeguard internal security extremely important. Specifically, Congress expressly set forth management's right to determine the "internal[-]security practices of the agency"[45] – which undoubtedly includes the right to establish information-security practices[46] – as one of the first management rights listed in the Statute. But, by the very act of including this provision in § 7106(a) of the Statute and making it subject to bargaining under § 7106(b),[47] Congress signaled that collective bargaining is wholly compatible with management's right to determine internal-security practices.[48] And while Congress instructed agencies (in FISMA) to protect federal information security, it also expressly included in the Statute an injunction to "safeguard[] the public interest"[49] and "contribute[] to the effective conduct of public business"[50] through the institution of collective bargaining. Although attaining both internal-security and collective-bargaining objectives may require planning and coordination, the laws at issue here (FISMA and the Statute) assign that responsibility in various ways to federal managers *and* their union counterparts.[51] In fact, Congress – by simultaneously finding both that the Statute "should be interpreted in a manner consistent with the requirement of an effective and efficient [g]overnment"[52] and that "labor organizations and collective bargaining in the civil service are in the public interest"[53] – clearly envisioned that the parties would collaborate to further their shared interest in a secure, safe, effective, and efficient government.[54] By finding sole and exclusive discretion based on the mere presence of internal-security considerations, the dissent would sacrifice the benefits that Congress intended collective bargaining to provide. And by suggesting that the Authority has "no . . . standing" to apply the Statute in cases that implicate other statutes, like FISMA,[55] the dissent ignores the responsibility Congress assigned the Authority to apply the Statute in the legally complex environment of the federal government. There can be no serious debate that the Authority not only can but also must interpret laws other than the Statute in resolving disputes.

Moreover, we note that the Arbitrator interpreted the parties' agreement as permitting "expedited implementation of new policies or practices"[56] in some situations. But in the circumstances of this case, the Arbitrator found the Agency's expressed security *concerns* were inconsistent with the Agency's *actions*, which the Arbitrator found "less than deliberate and speedy."[57] And given these actions – which included the Agency's allowing violations of its webmail policy for years, its waiting six months between deciding to block

[44] 124 Cong. Rec. 29,199 (1978) (statement of Rep. William D. Ford).
[45] 5 U.S.C. § 7106(a)(1).
[46] *See, e.g., AFGE, Local 1712*, 62 FLRA 15, 17 (2007) (noting Authority precedent holding that "proposals prescribing the actions management will take to ensure the security of its computer system" affect management's right to determine internal-security practices).
[47] 5 U.S.C. § 7106(b).
[48] *See* 124 Cong. Rec. 29,198 (1978) (statement of Rep. Ford) ("[T]he listed management rights [a]re to be narrowly construed exceptions to the general obligation to bargain in good faith . . . and . . . [§] 7106 [is to] be read to *favor collective bargaining* whenever there is a doubt as to the negotiability of a subject" (emphasis added) (internal quotation marks omitted)).
[49] 5 U.S.C. § 7101(a)(1)(A).
[50] *Id.* § 7101(a)(1)(B).
[51] *See* 124 Cong. Rec. 29,188 (1978) (statement of Rep. William Clay) ("[The Statute] imposes *heavy responsibilities* on labor organizations *and* on agency management." (emphases added)).
[52] 5 U.S.C. § 7101(b).
[53] *Id.* § 7101(a).
[54] *Cf. U.S. Dep't of the Treasury, Customs Serv., Wash., D.C.*, 59 FLRA 703, 708-09 (2004) (then-Member Pope concurring) (noting that § 7106 of the Statute "is a compromise between management's right to act within certain specified areas and the union's right to provide input into any decision affecting the conditions of employment of employees in its unit of exclusive recognition . . . . The intent is to ensure the effective and efficient operation of the [g]overnment consistent with the public interest in collective bargaining."); *U.S. Dep't of Transp., FAA, Standiford Air Traffic Control Tower, Louisville, Ky.*, 53 FLRA 312, 319 (1997) ("The definition of collective bargaining set forth in [§] 7103(a)(12) does not prescribe any particular method in which collective bargaining may occur. It is well[]recognized that collective bargaining may occur in a variety of ways, including the use of collaborative or partnership methods." (citations omitted)); *U.S. Dep't of the Army, Corps of Eng'rs, Memphis Dist., Memphis, Tenn.*, 52 FLRA 920, 932 (1997) (Member Armendariz concurring in part and dissenting in part) ("When Congress enacted the Statute, it recognized that labor organizations and collective bargaining promote an effective and efficient [f]ederal [g]overnment."); *U.S. Dep't of the Treasury, Customs Serv., Wash., D.C.*, 38 FLRA 770, 788 (1990) ("It is clear that . . . the Statute is to be interpreted in a manner consistent with an effective and efficient [g]overnment . . . . It is equally clear, however, that in enacting the Statute, Congress found that collective bargaining and the protection of employee and union rights is in the public interest.").
[55] Dissent at 12.
[56] Award at 38 (quoting CBA, Art. 9(F)).
[57] *Id.* at 39.

webmail and actually implementing the block, and its decision to un-block webmail for two months[58] – there is no basis for finding that, as a practical matter, the Agency actually was attempting to expedite its decision or that bargaining with the Union before implementing the change would have impeded any such attempts.

Finally, we note that the Arbitrator did not direct the Agency to restore employees' access to webmail, or to bargain over the substance of the change; he directed bargaining over only the impact and implementation of that change.[59] Thus, nothing in the award or our decision requires the Agency to bargain over proposals that actually conflict with law or government-wide regulation, including FISMA. Rather, we hold only that the Agency has not demonstrated that the cited provisions of FISMA foreclose bargaining *altogether*.

For the foregoing reasons, we conclude that the Agency has not established that the Arbitrator erred in finding that it lacked sole and exclusive discretion over the matters in dispute. Consequently, the Agency has not provided a basis for finding the award contrary to law.

V. Decision

We deny the Agency's exception.

[58] *Id.*
[59] *Id.* at 42-43.

Member Pizzella, dissenting:

I disagree with the majority insofar as they affirm an arbitrator's award that effectively undermines a key component of the Federal Information Security Management Act (FISMA)[1] – the responsibility for senior agency leaders "to *secure* their information and systems, identify and resolve current [information technology (IT)] *security weaknesses and risks*, as well as protect against *future* vulnerabilities and threats"[2] – unless they first bargain with the Union.

FISMA is a comprehensive and technical mandate that was enacted by Congress in December 2002 to confront the unique challenges posed by security threats to federal agency IT systems.[3] Since that time, two administrations,[4] six Congresses, and several federal courts[5] have reaffirmed the requirement for federal agencies – through their Agency heads, senior executives (typically "an executive at the Assistant Secretary level" or any other "senior management official or executive with authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals . . . [typically] an executive at the Assistant Secretary level"),[6] and key IT experts (whether those experts are called chief information officers (CIOs), or chief information and security officers (CISOs))[7] – to assume responsibility for ensuring the security of

[1] 44 U.S.C. §§ 3541-3549.
[2] Office of Mgmt. & Budget, Office of the President, OMB Memorandum M-03-19, Reporting Instructions for the FISMA & Updated Guidance on Quarterly IT Security Reporting (August 6, 2013) (OMB M-03-19), at 1 (emphasis added); *see also* Nat'l Inst. of Standards & Tech., Computer Sec. Div., Computer Sec. Res. Ctr., Frequently Asked Questions, FISMA FAQ 1, http://csrc.nist.gov/groups/SMA/fisma/faqs.html (last visited April 16, 2014) (NIST FISMA FAQs).
[3] *Trusted Integration v. United States*, 659 F.3d 1159, 1161 (Fed. Cir. 2011) (citing *Trusted Integration v. United States*, 93 Fed. Cl. 94, 95 (Fed. Cl. 2010)); *see also Federal Information Security: Current Challenges & Future Policy Considerations*: Hearing Before the H. Comm. on Oversight & Govt. Reform Subcomm. on Gov't Mgmt., Org. & Procurement, 111th Cong. (May 19, 2009) (statement of Vivek Kundra, Federal Chief Info. Officer, Adm'r for Elec. Gov't & Info. Tech., Office of Mgmt. & Budget, Exec. Office of the President) (Kundra Testimony).
[4] Office of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-10-15 FY 2010 Reporting Instructions for the FISMA & Agency Privacy Management (April 21, 2010) (OMB M-10-15); OMB M-03-19.
[5] *Cobell v. Kempthorne*, 455 F.3d 301 (D.C. Cir. 2006); *Cobell v. Norton*, 394 F. Supp. 2d 164, 173 (D.D.C. 2005); *Trusted Integration v. United States*, 659 F. 3d at 1159.
[6] *Cobell v. Norton*, 394 F. Supp. 2d at 173.
[7] *Id*.

federal IT systems and to identify and eliminate risks to those systems.

Former Federal Chief Information Officer, Vivek Kundra, noted in testimony before Congress that "the security of [f]ederal information systems [remains] a major concern [because the] nation's security and economic prosperity depend on the stability and integrity of our [f]ederal communications and information infrastructure".[8] And the dangers are not merely hypothetical. From the inception of this dispute (in September 2008)[9] until its arbitration (in September 2012),[10] federal computer systems were subjected to at least fifty-one "[s]ignificant [c]yber [a]ttacks,"[11] including those documented at the: CIA (June 2011); U.S. Senate (June 2011); Department of Commerce (February 2012, December 2009); Department of Defense (February 2012, December 2011, July 2011, December 2010, April 2010, December 2009, and November 2008); Nuclear Security Agency (October 2011); Department of Energy National Laboratories (July 2011 (2 locations) and April 2011); Department of Homeland Security (DHS) (February 2012, May 2009); Department of Interior (May 2010, November 2009); Department of Justice (January 2012); Federal Bureau of Investigation (February 2012, January 2012, June 2011); Department of Transportation (June 2010 and July 2009); Federal Aviation Administration (May 2009); Department of Treasury (July 2009); and National Aeronautics and Space Administration (November 2011, May 2011 (2 incidents), March 2011).[12]

After these, and other, "successful breaches,"[13] the Office of Management and Budget (OMB) determined that more "[c]onsistent, cost-effective application of security controls across the [f]ederal [g]overnment"[14] was required to "enable" agencies to exercise responsibility to make "timely decision[s]" that address the unique "risk[s]," "vulnerabilities," and "threats" to their IT systems.[15] It is apparent, therefore, that FISMA designated senior leaders, who possess the necessary expertise, the responsibility, and the sole discretion to determine what steps are required to address security risks to their agency's IT systems and how to comply with all other FISMA requirements.[16]

In this case, the Agency has a mere thirty-six employees to monitor an IT system that is used by 30,000 employees deployed around the globe.[17] During the four years that cover this grievance, the Agency experienced daily malware attacks[18] (not unlike those inflicted on other federal agencies as noted above).[19] Despite repeated warnings from senior Agency officials and ongoing training efforts, a significant "uptick in mail infections and privacy spills" occurred in February 2011.[20] The Agency determined that the "uptick" resulted primarily from employees accessing personal webmail accounts on their work computers.[21]

[8] Kundra Testimony (May 19, 2009).
[9] Award at 6.
[10] *Id*. at 14.
[11] *See* Paul Rosenzweig, *Significant Cyber Attacks on Federal Systems – 2004-Present*, Lawfare, (May 7, 2012) http://www.lawfareblog.com./2012/05/significant-cyber-attacks-on-federalsystems-2004-present.
[12] *Id*.
[13] Kundra Testimony (May 19, 2009).
[14] Emerson Boyer, *What FISMA Means to You*, Federal IQ, (October 31, 2012) http://fediq.com/fisma-defined/.
[15] OMB M-10-15 at 1.

[16] *Cobell v. Kempthorne*, 455 F.3d at 313-14. The majority notes, as if it is a remarkable event, that the district court's opinion in *Cobell v. Norton* was "vacated" and that the specific issue before the United States Court of Appeals for the District of Columbia Circuit (D.C. Circuit), at that stage did not directly concern "FISMA compliance." Majority at 5. That much is true. The D.C. Circuit simply vacated the district court's order insofar as it ordered injunctive relief against the agency. The majority misses the point, however, that the D.C. Circuit unmistakably and favorably embraced the district court's review of the history and requirements of FISMA and the responsibilities that FISMA places on "the head of each agency," *Cobell v. Kempthorne*, 455 F.3d at 313-14, the matter which is central to the issue before us in this case. C*ompare Cobell v. Norton*, 394 F. Supp. 2d at 170 (FISMA requires that agencies "develop, document, and implement an agencywide information security program") (quoting 44 U.S.C. § 3544)); *id*. at 171 (each agency is required to implement "a minimum set of security controls" (quoting OMB Circular A-130, App. III (internal quotation marks omitted) and provide "minimum information security requirements)) (quoting 40 U.S.C. § 11331(a)(1))); *id*. at 172 (security accreditation is "official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risks to agency operations, agency assets, or individuals" (quoting Ron Ross, Marianne Swanson, et al., Information Security: Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, at 1 (May 2004), United States Department of Commerce, National Institute of Standards and Technology, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf. NIST FISMA FAQs, Q.2 (the ultimate objective of the Risk Management Framework is to enable agencies to conduct day-to-day operations of the agency); OMB M-10-15 at 1 (CIOs, CISOs, and other agency management all need to have different levels of information to enable timely decision making).
[17] Award at 5.
[18] *Id*.
[19] *See supra* 10-11.
[20] Award at 8.
[21] *Id*.

As a consequence, the Agency notified all employees that they would "no longer be able to access personal webmail accounts on any [Agency] network."[22] The Union, however, "demanded that the Agency maintain the status quo ante until bargaining [was] concluded."[23] The Agency refused to negotiate because its decision to terminate access to personal webmail accounts on Agency networks was an exercise of its "right to determine its internal security practices under 5 U.S.C. § 7106(a)(1)"[24] and was within its "sole and exclusive discretion" to reduce risks to its IT systems under FISMA.[25]

The Arbitrator devotes just seventy-five words[26] to reject the Agency's arguments – concerning the security threats it faced and what actions FISMA required[27] –that it exhaustively detailed over two days of testimony, through 622 pages of transcript,[28] and in an eighty-eight page brief.[29] The Arbitrator, nonetheless, determined that "nothing in the FISMA statute . . . provides [the Agency sole and exclusive] discretion" to "implement[] policies and procedures to cost-effectively reduce risks [in its IT systems] to an acceptable level" *unless the Agency first provides the Union with an opportunity to bargain*.[30] The Arbitrator effectively determined, and my colleagues agree, that the Agency may not take *any action* to reduce security risks to its IT systems, *without first providing the Union an opportunity to bargain*, simply because Congress did not include language in FISMA that is "similar to any statutory wording that *the Authority or the courts* have previously *recognized as conferring* sole and exclusive discretion" upon a federal agency.[31]

The D.C. Circuit does not agree with my colleagues. To the contrary, the Court noted that FISMA makes the head of each agency responsible for "providing information security *protections* commensurate with the risk and magnitude of the harm resulting *from unauthorized access, use*, disclosure, disruption, modification, or destruction,'"[32] for "develop[ing], document[ing], and implement[ing] an agency-wide information security program,"[33] and for "ensur[ing] compliance with information security standards promulgated by the Department of Commerce."[34] The Court also acknowledged that "a role for the judicial branch" is "[n]otably absent" within FISMA's "multi-layered statutory scheme" and doubted "that courts would ever be able *to review* the *choices an agency makes* in carrying out its FISMA obligations."[35]

It is obvious to me (after having served for seven and a half years as the CIO at the U.S. Department of Labor) that neither the Authority nor the Arbitrator possesses the specialized knowledge or expertise that would permit us to decide when a federal agency ought to address specific security risks or permit us to second guess how that agency should exercise those responsibilities. Under FISMA, those determinations are left to the agency's senior leadership and technical experts, in consultation with the recognized experts at OMB and the Department of Commerce's National Institute of Standards and Technology (NIST), who actually possess the necessary expertise to "push"[36] federal agencies to make "timely decision[s]"[37] that will minimize "their risks and make substantial improvements in their security."[38] From my perspective, it is a huge stretch to presume that the organic provisions of our 20th-century Statute that were implemented prior to the advent of the internet, could effectively preempt the flexibilities and obligations that were specifically imbued to federal agency executives under the focused, 21st-century provisions of FISMA in order to address the threats that occur in real-world security to federal IT systems.[39] My colleagues disagree with me, but they alone must answer for their expansive view of our Statute (which they apparently believe to be without limit)[40] to these unique circumstances. From my perspective, the Authority has no more standing to tell the D.C. Circuit, OMB, or the Department of Homeland Security what steps the Agency must take to fulfill its responsibilities under FISMA than the Authority had to tell the Department of Homeland Security's Office of

[22] *Id.* at 10 (quoting Hr'g Tr. at 516-20; Agency Ex. 20) (internal quotation marks omitted).
[23] *Id.* at 13 (quoting Jt. Ex. 6 at 2) (internal quotation marks omitted).
[24] *Id.* (internal quotation marks omitted).
[25] *Id.* at 27-28.
[26] *See Id.* at 28.
[27] Exceptions at 3-6; *see also* Hr'g Tr. at 1-623; Agency's Closing Brief at 1-88.
[28] Exceptions, Attach. 2 (Hr'g Tr).
[29] Exceptions, Attach. 3 (Agency's Closing Brief).
[30] Award at 28 (internal citations omitted).
[31] Majority at 4-5 (emphases added).
[32] *Cobell v. Hempthorne*, 455 F.3d at 313 (emphases added) (internal citation omitted).
[33] *Id.*
[34] *Id.*
[35] *Id.* at 314 (emphases added).
[36] OMB M-10-15 at 2.
[37] *Id* at 1.
[38] *Id.* at 2; *see also Cobell v. Hempthorne*, 455 F.3d at 313.
[39] *See U.S. Dep't of Treasury, U.S. Customs Serv. v. FLRA*, 43 F.3d 682, 689-90 (D.C. Cir. 1994) (Treasury) ("The very preclusion of judicial review suggests powerfully that Congress could not have contemplated, let alone intended, that all or any part of American law would be definitively interpreted by the FLRA on review of one or a series of cases originally put to arbitration. To give any administrative tribunal such final authority to construe any or all statutes or treaties of the United States would be a staggering delegation, which surely would have provoked considerable congressional debate.")
[40] *See* Majority at 7.

Inspector General how it should exercise its statutory responsibilities under the Inspector General Act of 1978,[41] to tell the Department of the Navy how it should spend its money,[42] or to tell the National Labor Relations Board how it should interpret the National Labor Relations Act.[43]

Therefore, unlike my colleagues, I cannot conclude that Congress intended for our Statute to be read so expansively as to impose additional – in this case bargaining – requirements on federal agencies *before* they can act to secure the integrity of their federal IT systems, the breach of which, could directly impact "[o]ur nation's security and economic prosperity."[44] And, to the extent a federal agency's discretion to address IT security risks is limited, in any respect, it is limited by the policies and recommendations of recognized experts at OMB and NIST[45] and not by a generic and unrelated statutory construct such as our Statute.[46] Those experts, including those at DHS, established specific responsibilities for federal agencies with which federal agencies are required to comply.[47] The district court in *Cobell v. Norton* [48] and the D.C. Circuit in *Cobell v. Hempthorne*[49] identify at least six such responsibilities.

As the majority concedes, statutes need "not use any specific phrase or words in order to confer sole and exclusive discretion."[50] And while I agree with my colleagues that the absence of wording *in many circumstances* would indicate a "strong indication that Congress did not intend the [agency] to have unfettered discretion" over a particular matter,[51] the history, and implementation, of FISMA (as interpreted by at least four federal courts, OMB, and NIST),[52] as well as the real-world threats faced by federal agencies every day, do not lend themselves to an indication of that intent.[53] Imposing on the Agency an obligation to bargain, under these circumstances, is akin to applying the trouble-shooting guidelines from the owner's manual of a 1978 IBM desktop PC to a 2012 Apple MacBook Pro.

To the contrary, the authorities noted above indicate that FISMA is a unique Statute – focused on protecting the Federal Government's IT infrastructure – that requires leaders, who possess relevant technical expertise, to make decisions and take specific actions when faced with security threats.

Therefore, I would conclude that the Agency has sole and exclusive discretion to terminate access to personal webmail accounts on Agency computers when faced with specific security threats and that it was not obligated to bargain with the Union before it could take that action.

Thank you.

---

[41] *U.S. DHS, U.S. CBP v. FLRA*, No. 12-1457, 2014 U.S. App. Lexis 10231 (D.C. Cir. June 3, 2014).
[42] *U.S. Dep't of the Navy v. FLRA*, 665 F.3d 1339 (D.C. Cir. 2012).
[43] *NLRB v. FLRA*, 613 F.3d 275 (D.C. Cir. 2010).
[44] Kundra Testimony (May 19, 2009).
[45] OMB has also enlisted the Federal CIO Council, the Council of Inspectors General on Integrity and Efficiency, the Information Security and Privacy Advisory Board, the President's Cybersecurity Coordinator, the Government Accountability Office, and the DHS (of which the agency is a component) to suggest strategies to reduce risks and make improvements. OMB M-10-15 at 2.
[46] *U.S. Dep't of the Navy, Naval Undersea Warfare Ctr. Div., Newport, R.I. v. FLRA*, 665 F.3d 1339, 1348 (D.C. Cir. 2012) (Authority entitled to no deference when it "endeavor[s] to reconcile its [own] statute with another statute . . . 'not within its area of expertise'") (internal citations omitted)); *see also U.S. Dep't of Treasury,* 43 F.3d at 689-90.
[47] OMB M-10-15 at 2.
[48] 394 F. Supp. 2d at 170-78.
[49] 455 F.3d at 313-14.
[50] Majority at 4 (quoting *U.S. Dep't of the Interior, Bureau of Indian Affairs, Sw. Indian Polytechnic Inst., Albuquerque, N.M.*, 58 FLRA 246, 248 (2002)).
[51] *Id*. at 3 (quoting *Dep't of VA, VA Med. Ctr., Veterans Canteen Serv., Lexington, Ky.*, 44 FLRA 162, 165 (1992).
[52] *See supra* notes 2-6, 13, 16.
[53] *See supra* n.39.