Federal Aviation Administration

Memorandum

Date: May 24, 2011

To: Senior Vice President, ATO Finance
Vice President, Technical Operations
Chief Information Officer, FAA

From: Chief Information Officer, ATO

Subject: Applications for Waiver to FAA Internet Access Point (IAP) Policy

Attached is the *Applications for Waiver to FAA Internet Access Point (IAP) Policy* with supporting documentation.

The application has been approved, and signatures are required to complete the process, as per Appendix A and Appendix B.

After signing, please call Audra Backaitis, ext. 77203, to pick up the packet.

Should you have any questions, please call Richard Boe at ext. 77203.

Appendix A
Justification for Internet Access Point Request

The following are the minimum requirements necessary for you to gain FAA certification and authorization of an Internet Access Point (IAP). You must gain a waiver and to do that you must first write a Justification for Internet Access Point for evaluation and approval by the appropriate AO.

(1) Explain in detail why you need a source of access to the internet in an FAA facility other than those already provided by the FAA.

(2) Explain your need for an IT infrastructure separate from the FAA.

(3) Demonstrate your financial ability to establish and support the IT infrastructure IAW the ATO Waiver process.

(4) Demonstrate that you have the available technical capacity to install and maintain an IT network that won't damage or interfere with the FAA infrastructure.

(5) The following signatures are required on all Justification of Internet Access Point Requests.

Chief Information Officer, ATO

Senior Vice President, ATO Finance

Vice President, Technical Operations Services

AFL-CIO

February 14, 2011

Richard Boe
Federal Aviation Administration
800 Independence Avenue, SW
Washington, DC 20591

Cert # 7009 0960 0000 1590 3740

Re: Independent Internet Access Points

Dear Mr. Boe:

I am writing regarding NATCA's request to install independent internet access points ("IAP") and separate IT infrastructures-owned, operated and maintained solely by NATCA- in FAA facilities. As background, in October 2008, the Union requested that the Agency allow additional local facilities to install independent access points, in the form of NATCA-controlled broadband or wireless servers, in NATCA union offices. There are distinct internet connections already established by NATCA within FAA facilities. These existing connections have been established through the necessary labor-management coordination, and are considered "approved" and appropriate. The practice between the parties has always been to allow the Union to pay for the installation and maintenance of such systems without any oversight by the FAA. When the Union made its most recent request for additional local facilities to install IAPs, the FAA denied the Union's requests at the local level. At the national level, the Agency expressed security concerns regarding the use of any non-FAA run or monitored system, and in November 2008 the FAA threatened to remove all existing Union computer systems and networks. During the course of negotiations for the 2009 Collective Bargaining Agreement, however, the FAA agreed to cease any efforts to remove any existing systems until the Parties reached an agreement concerning computers and internet systems. On June 24, 2010, the Agency provided an IT Infrastructure briefing to NATCA. While the Parties did not reach a resolution regarding the applicability of the unilaterally developed waiver process to Union computers and networks in FAA facilities, NATCA is ready to attempt to navigate the waiver process in attempt to install additional IAPs into FAA local facilities.

According to the FAA's own Air Traffic Organization Policy (N JO 1370.45), there are several minimum requirements necessary for one to gain FAA certification and authorization of an IAP. In order to gain a waiver to maintain an IAP, one must first write a justification for internet access point request for evaluation and approval by the Agency. NATCA submitted a justification for internet access point request on February 2, 2011. On February 10, 2011, the Agency, in the person of Roscoe Ridley, informed NATCA that it had reviewed NATCA's IAP Waiver Justification Request and found it supportable from the technical aspects, and that NATCA was able to move forward with completing the waiver process. The following represents NATCA's official internet access point waiver request pursuant to (N JO 1370.45, Appendix B)

Explain in detail why you need a source of access to the internet in an FAA facility other than those already provided by the FAA.

The Union requires a source of access to the internet in all FAA facilities that is separate and distinct from that which is already provided by the Agency for various reasons. First, and foremost, the Union has a distinct interest in protecting its members, representatives and any information used by its representatives to carry out their functions. NATCA representatives rely heavily upon the internet to engage in the representation of bargaining unit employees. Facility representatives frequently use the internet to query various databases, conduct legal research, send emails, and prepare for oral presentations, hearings and the like. Any information used by NATCA, on the employee's behalf, should be confidential. In fact, the use of FAA controlled internet access points creates the potential for a lapse in privacy, and could thereby undermine the representative in carrying out his or her statutory obligation to properly act on behalf of the employee. The Union has raised its concerns in the past regarding three separate security breaches- in February 2009, May 2009, and February 2010-containing the personal identity information of employees. The Agency also has an interest, undoubtedly, in siphoning misconduct as it relates to computer and/or internet misuse. While NATCA intends to abide by all rules, regulations and policies pertaining to internet usage at FAA facilities, there is the possibility that the Agency may target NATCA representatives and/or employees for discipline if allowed the role of oversight of internet access. NATCA does not find the Agency's unfettered access to the Union's internet usage, particularly as it relates to Union activities, appropriate and therefore find the need for an independent internet access point warranted.

From a legal standpoint, an independent internet access point is necessary to uphold the sanctity of NATCA as an independent entity that operates as the exclusive representative of all bargaining unit employees within the scope of the various FLRA-certified bargaining units. The Federal Service Labor-Management Relations Statute ("FSLMRS" or "the Statute") prohibits an Agency from taking actions that sponsor, control, or otherwise assist any labor organization, other than to furnish, upon request, customary and routine services and the facilities. 5 U.S.C. Section 7116(a)(3) prohibits the sponsorship, control and assistance of the union. When considering whether an agency action runs afoul of this prohibition, the Federal Labor Relations Authority will consider whether or not the support provided by the Agency constitutes "company unionism." *Social Security Administration and National Treasury Employees Union and American Federation of Government Employees*, 52 FLRA 1159, 1176 (1997). 5 U.S.C. Section 7116 closely mirrors section 8(a)(2) of the National Labor Relations Act. The purpose of both statutory provisions is to "preserve the bargaining unit representative's independence." The FAA's offer to provide the Union with FAA-sponsored and controlled internet undermines the Union's independence and serves as a breach of this statutory obligation to maintain an "arms-length" relationship between the employer and the Union. NATCA representatives rely heavily upon the internet to engage in the

representation of bargaining unit employees. Because of the scope of this reliance, any internet access points or systems provided and maintained by the FAA would constitute more than a de minimis routine service or facility.

Explain your need for an IT infrastructure separate from the FAA.

NATCA maintains several databases and computer systems that are available to all facility representatives. These systems- a membership information database and a grievance tracking system, specifically-are the property of the Union. One system, the grievance tracking system, is owned, operated and maintained exclusively by the Union. The grievance tracking system contains various information related to individual grievances across the country. Some of this information is evidence that will be used by Union advocates to represent the employee through various stages of the negotiated grievance process, including arbitration. Not only does the Union have a proprietary interest in this system, but it has a representational duty to maintain the sanctity of all information related to the grievance procedure process, and any information contained in the grievance tracking system. Using the same IT infrastructure as the FAA undoubtedly compromises the Union's ability to protect this information. In fact, the law is settled that employees have no reasonable expectation of privacy when using an agency computer system. *Office of Justice Programs*, 105 LRP 53296 , 60 FLRA 124 (FLRA 2004).

Another bone of contention between management and labor has been the extent to which computers can be used to measure employee performance and conduct. NATCA has a legitimate concern that employees may be disciplined for any information retrieved from his or her computer usage-even if used in the performance of his duties as union representative. There is an ample amount of jurisprudence that establishes that when an employee is using the Agency's IT infrastructure nothing precludes management from using a particular method of monitoring that employee's work performance. In fact, such action is justified as a management right under section 7106(a)(2)(A) and (B) of the Statute. *American Federation of Government Employees, Local 2879 and U.S. Department of Health and Human Services, Social Security Administration, Chula Vista District, San Diego, California*, 38 FLRA 244, 247-48 (1990). See also, *National Federation of Federal Employees, Local 1482 and U.S. Department Of Defense, Defense Mapping Agency, Hydrographic / Topographic Center, Washington, D.C.*, 44 FLRA 637, 665-70 (1992) (Hydrographic / Topographic Center) ("Proposals that prohibit management from using information derived from its computer system to monitor employee production have been held to directly interfere with these rights.") In order to maintain some autonomy over the resources and representational activities of NATCA it is, therefore, necessary to maintain a computer and internet infrastructure that is separate and distinct from the Agency's.

The member-information system is also owned by NATCA, but is provided by a third party contractor. Since NATCA owns the system, it has purchased NATCA-specific licenses for various modules including, but not limited to, membership and finance, as well as a member-portal. NATCA pays a fee for these modules and the protections associated with the services provided by the contractor. NATCA's purchase of these safeguards is essentially rendered useless if the Union must access this system through the Agency's IT infrastructure and computer system. As mentioned above, regarding the GATS system, NATCA has the same personal and proprietary interest in protecting all information contained in the membership database as well. NATCA has gone to great lengths to ensure that the members' personal and financial information is protected from any external infiltration that might put the members' information at risk. The Union's interest in protecting the sanctity of the grievance system database and the membership database necessitates an internet and computer infrastructure that is owned, operated, and maintained solely by NATCA.

Demonstrate your financial ability to establish and support the IT infrastructure

NATCA represents over 15,000 bargaining unit employees, and has a consistent stream of income through the dues received by its members and associate members. The Union's various local organizations have steady income that is monitored and approved by the Union's National Finance Committee. This serves as an additional income stream and asset as well. NATCA operates as a labor organization with all financial records and dealings monitored in accordance with the Department of Labor's protocols and regulations. As such, the Union is capable of providing each of its local organizations with the technical and financial resources to establish and maintain an IT infrastructure, including a successful independent internet access point.

Demonstrate that you have the available technical capacity to install and maintain an IT network that wont damage or interfere with the FAA infrastructure.

In February 2009, the FAA submitted a letter to NATCA, c/o Kevin Sills, denying the Union's request for its own internet access point and IT infrastructure within FAA facilities, most notably because of the suspicion that it would compromise the highly sensitive information already contained in the FAAs IT network. The Agency argued that the existence of an independent IAP might allow for the inadvertent infiltration into the FAA's system. The Agency also stated that pursuant to Article 23.1 of the CBA, all Agency computers and information systems must be protected in accordance with the Computer Security Act of 1987 and FAA Order 1370.82 and .83. Although the FAA has expressed some theoretical concerns with the FAA's IT infrastructure being damaged by allowing NATCA to have its own IT infrastructure, the FAA has never cited any instance of a security breach, or any problem at all with any existing internet connection or NATCA-run IT network. In fact, NATCA has concerns of its own about having a sound

IT network, separate and distinct from the FAA, and ensuring that all security protocols, rules and regulations are followed.

In effort to protect the FAA infrastructure, as well as its own, NATCA is willing to install any computer firewalls, virus protection, and/or password protection in order to ensure that the FAA system is not compromised or damaged. The Union is also prepared to adopt the provisions and operating procedures of the FAA's ATO Wireless Implementation Policy. To that end, the Union will establish both physical and electronic impediments, to include technology such as MAC filtering, to access by authorized individuals. The physical and electronic barriers will preclude any individual employee (management or bargaining unit) from making unauthorized connections to the Union's internet access points. As such, the Union-controlled system will be entirely separate from the FAA's infrastructure. No individual will be able to attach an FAA computer to the Union-controlled system. For facilities where there is dedicated office space for the Union, the Union will establish a secure location to maintain all internet and computer systems. For those facilities with shared office space, the Union will operate and maintain a physical barrier to unwanted access. The Union will operate the current technology that enables encryption of data used on an internet system. To that end, the Union will, at a minimum, engage an administrator for the internet and computer systems of the Union's choice at each facility to limit the access to and by bargaining unit employees. As an entity authorized to use and maintain its own IAP, NATCA fully intends to maintain its own IT infrastructure to a level consistent with FAA standards, federal regulations and policies. Upon request, the Union at the local level shall provide a MAC address listing to the Agency for that given network. The provided MAC address listing shall only be used to verify that the integrity of the FAA's network is not being compromised.

Based on the following arguments, NATCA believes it has proven that it meets the minimum requirements necessary to gain FAA certification and authorization of an IAP. At this point, the Union requests that the appropriate parties (i.e. the ATO CIO and the Line of Business AO) evaluate this "Justification for Internet Access Point" and provide the necessary approvals to use the waiver process.

Sincerely,

Kimberlee Gee

Kimberlee J. Gee, Esq.
Labor Relations Staff Representative