Q & A on Internet and Wi-Fi Access at Job Corps Centers

Q: **What can be done to address the issue of limited bandwidth on Job Corps centers? We cannot use Internet-based curricula due to bandwidth limitations on center.**

A: As indicated in Job Corps Date Center (JCDC) Notice 12-089, one option that centers have for increasing available bandwidth on center is to contract with a local provider for a cable modem. Center Operators would bear the costs for this.

As outlined in the above referenced notice, the requirements for the installation of cable modems are as follows:

Requirements

- The Job Corps center must procure business-class cable modem Internet service with a static Internet Provider (IP) address. Dynamic or Dynamic Host Configuration Protocol (DHCP) IP addressing is not allowed for this service.
- The Job Corps center is responsible for all installation charges, monthly recurring charges and maintenance fees associated with the circuit.
- The circuit must be installed in the network closet which houses the JCDC-provided routers, and the cable modem must be connected to the interface on the router using an ethernet cable.
- All current Job Corps security and Internet filtering policies will be applied to this service.
- The Job Corps centers' Information Technology Point of Contact (IT POC) are responsible for coordinating maintenance activities with the service provider, and will contact their technical support in case of any problems with the service. JCDC will not open service requests with a third party Internet service provider.
- The Job Corps center IT POC will provide the details of the Internet service which provides details such as static IP address, subnet mask, Domain Name Server's address, and circuit identification number to JCDC Helpdesk before service activation and installation.
- The Job Corps center IT POC will notify JCDC by opening a helpdesk ticket if this circuit fails, or Internet access is unavailable to troubleshoot further and determine the cause of failure.
- Per Department of Labor Management System 9, Chapter 1200, Department of Labor Safeguarding Sensitive Data Including Personally Identifiable Information - January 8, 2008: Any information technology device (mobile or stationary) used to access or store protected personally identifiable information and other sensitive data must either be the property of the government or government-authorized or leased, and must be configured to meet the requirements of this and other applicable policies. The Job Corps center will only be allowed to connect government-furnished equipment to the network to access Internet services. This option is not intended for personally owned internet capable devices.
- The service should be IPv6 capable now or in the near future.
- Currently 39 Job Corps centers have procured cable modems and stated that performance has improved.

Q: **Why doesn't JCDC procure cable modems for the centers?**

A: JCDC can only provide circuits that are procured via the federal Networx contract. The charge rate is much higher than most local Internet service providers. Circuit orders via the federal Networx contract also take significantly longer times to process. Local Internet service providers can provide additional high speed bandwidth, with quicker install times, and lower monthly costs to the center.

Q: **Can we have separate student/staff networks?**

A: Job Corps currently separates the student from the staff network.

Q: Can the Job Corps Citrix servers at JCDC be upgraded to support the demand for better service?

A: Yes, we are already doing this. We have upgraded more than 200 servers to support Citrix. A new version of Citrix is to be piloted at several centers in the next few weeks; rollout to additional centers will follow, assuming there are no issues.

We currently are using version 4.5 of Citrix XenApp. We will migrate all users to Citrix XenApp 7.6 in the coming months.

Q: Why do center systems slow down when multiple users are online?

A: This occurs because of bandwidth limitations at the center level. We are already working toward this goal of increasing the bandwidth at the centers, but it takes time and funding. Often, the center's infrastructure needs to be upgraded before higher speed connections can be installed.

We are currently piloting the use of 10 Mbps Multi-Protocol Label Switching (MPLS) circuits and replacing multilink T1s. Upgraded MPLS circuits have been installed at Sierra Nevada and Turner Job Corps centers, and are currently being monitored for performance. We have 10 additional pilot installations of 10 MB MPLS circuits pending. After reviewing the results of the pilot, a survey schedule will be provided for determining centers' wiring needs, and MPLS circuit upgrades.

Q: Why does having multiple users online slow down the Center Information System?

A: The issue is not with CIS, but with the amount of bandwidth available at the center level. We are already working toward this goal of increasing the bandwidth at the centers.

Q: Can center T1s be replaced with fiber connections or high speed Digital Subscriber Line (DSL)?

A: We are already working toward this goal, but it takes time and funding. Often, the center's infrastructure needs to be upgraded before higher speed connections can be installed.

Q: Job Corps bulk and group policy updates drastically slow down the network; why can't intermediate servers be put on centers to serve as a cache for these updates and improve performance?

A: We are currently reviewing options, such as read-only domain controllers; we are implementing ForeScout to replace McAfee NAC.

The Department of Labor (DOL) has mandated the use of Tivoli Endpoint Manager (Bix Fix) to provide a standardized mechanism to push out software patches and security updates as well as report security compliance levels of all hardware and software assets in the department. DOL mandates strict time guidelines for the implementation of software patches and updates based on severity of the problem.

Below is an excerpt from the DOL Office of the Chief Information Office (OCIO) regarding the required timelines for installing patches and updates:

- *OCIO Security reserves the right to specify a minimum level of importance (including but not limited to, minimum requirements) for updates that have been released by approved sources. In instances where OCIO Security does not specify minimum requirements for updates, information system personnel shall develop, implement, and comply with any and all agency requirements. The minimum requirements for installing updates on information systems are as follows:*

  a. *Updates identified as critical importance (including all out of cycle updates) must be installed within 72 hours of release.*

b. *Updates identified as high importance must be installed within 5 business days of release.*
c. *Updates identified as moderate importance must be installed within 10 business days of release.*
d. *Updates identified as low importance must be installed within 20 business days of release.*

Q: JCDC Security requirements interfere with our students getting access to education Web sites and social media. Why can't the network be more open?

A: Security requirements for the Job Corps network are not the invention of the JCDC, but Office of Management and Budget/Federal Information Security Management Act, that have imposed not just on Job Corps but on other government systems as well.

There has been discussion about opening up access to social media sites after training hours. To date, the National Office has not established requirements.

Centers should provide JCDC with a list of any blocked educational sites; JCDC can assist with opening any blocked educational content. Please contact the JCDC helpdesk, helpdesk@jobcorps.org, regarding this issue.

Q: Are student groups permitted the use of Wi-Fi on center if they monitor the system and pay the monthly fees? Students use their personal electronic devices (not government computers), and do not access the Job Corps network.

A: It is possible to create a backdoor into the Job Corps network using hotspots. There is no way to tell what potential vulnerabilities exist on non-government furnished equipment. Wi-Fi hotspots are not allowed for use on the Job Corps centers, as they are considered non-managed third-party circuits. Centers may purchase cable modems for additional bandwidth per JCDC Notice 12-089.

Q: Wi-Fi is used in the Academy Director's office--for visitors who need to use the Internet. Is this permissible? Government computers are not used on this Wi-Fi and the Job Corps network is not able to be accessed.

A: The guest Virtual Local Area Network should be used for these purposes. If the center does not have a wireless Access Point (AP) to support this network wirelessly, JCDC will be providing wireless APs for Job Corps network connectivity in the near future. A notice is forthcoming with more information regarding wireless AP deployment.

Q: Why do staff/students have to enter multiple passwords to access the cloud, network and their PCs?

A: On the Job Corps domain, users may have to authenticate multiple times (if going from Citrix, to a Career Development Services System application, to an Internet site, for example), but the password is the same throughout.

Q: Center IT POCs often struggle to keep up with new software or network upgrades in addition to their center responsibilities. Additionally, IT POCs have limited rights to make network administrative decisions. Can more IT POC staff positions be funded?

A: The National Office has discussed the feasibility of hiring up to two IT POCs per region who would be trained by JCDC and report to JCDC, in order to take some of the load off center IT POCs so that they (center IT POCs) can focus more on their center responsibilities. Funding was previously unavailable to satisfy this request.

The Job Corps National Office enforces centralized management of network and user account administration to ensure consistent implementation of Office of Management and Budget- (OMB) and DOL-mandated security policies across all 125 Job Corps centers. Prior decentralization of these functions allowed widely varying levels of compliance with policies which resulted in audit findings against Job Corps from the Office of the Inspector

General. DOL constantly monitors all agencies within the department for compliance to security policies, which are subsequently reported to OMB and Congress. As a result, the Job Corps National Office will continue to enforce centralization of these functions to ensure the highest level of compliance.

Q: When are thin clients being replaced? Aren't most of them at end of life?

A: Job Corps is in the process of procuring and replacing end-of-life thin clients.

Q: Why doesn't the data center purchase printers for the centers?

A: The centers have been responsible for purchasing their own printers. Please see the link below for a list of recommended printers from Citrix. The centers can also contact the helpdesk for guidance on printers to purchase, and help troubleshoot any printing issues.

http://support.citrix.com/servlet/KbServlet/download/10498-102-649930/HPprinters_CitrixXenApp_1053.pdf