## Q & A Policy Issuance 06-07

Network Security Protocols

**Issuance 06-07**

**Q** It is my understanding that the FISMA audit finding(s) are directed to DUA and the integrity of UI data and records? How do the findings pertain to the Career center system?

**A** Yes, the audit and its findings are directed at DUA, and at UI records and data. However, the findings apply to the network known as etma.org, which is the network for all Career Center staff affected by this policy issuance. The policies and procedures required for adoption as delineated in MassWorkforce Issuance 06-07 are "best practices" for securing any IT network, including the full detma.org network, from unauthorized and inappropriate use.

---

**Q** Is it essential that the same level of security be extended to all DCS networked systems?

**A** Since there are is only one DCS networked system, 'detma.org', the answer is yes, and all communication with every device on the detma.org' network is now subject to the policy described in MassWorkforce Issuance 06-07 and any future security protocol requirements. If DCS operated another network system distinct from detma.org, DCS would have an opportunity to establish an alternative policy regarding the level of network security and the specific protocols it wanted to observe in order to conform that network's traffic. However, this is not the case with 'detma.org'. since it is a common shared network.

---

**Q** Can some sort of "firewall" between DCS and DUA be built that safeguards UA information and still allows DCS to service its customers effectively?

**A** Nothing in the policy restricts the ability of staff to provide effective services to customers. The issuance describes policies that must be followed to assure the integrity of the personal data of UI claimants and other workforce system customers made available through and shared by DUA and other workforce development personnel (including staff of DCS, One-Stop Career Center Operators and other local workforce system partners). This data is available through the 'detma.org' network, on which MOSES and other workforce system applications utilized by One-Stop Career Center customers reside.

---

**Q** Many non-DWD sites run "sensitive" software (e.g. MOSES) on their own networks. How do the policies delineated in MassWorkforce Issuance 06-07 apply to those users?

**A** The policies apply to each device connected to the 'detma.org' network. They do not apply to any device that is not connected to the 'detma.org' network. If a device is connected to 'detma.org', the policies delineated in MassWorkforce Issuance 06-07 (as well as future network security related policies) are applicable.

It should also be noted that such non-DWD sites running MOSES and/or other DCS administered workforce applications through the 'detma.org' network are subject to the confidentiality safeguard requirements delineated in WIA Communication 05-76 Policy to Protect Confidential Information (10/19/2005), including signing and submitting the required Confidentiality Policy Form for those staff who may access confidential customer information through MOSES or other applications connected through the 'detma.org' network.

---

**Q** Are there "security" risks with those non-DWD site users and how is the risk managed with those users by the DWD IT Dept.?

**A** As cited above, the same policies and procedures apply to every device connected to detma.org. Immediate notification of known or suspected security 'risks" associated with non-DWD sites attached to detma.org must be made promptly and in writing to:

Jeff Ritter
Associate Director for Information Technology
Charles F Hurley Building
Boston, MA 02114

All pertinent documentation must also be provided with the notification in order to initiate an investigation of any such potentially serious situation.

---

**Q** The more rigorous security procedures described in MassWorkforce Issuance 06-07 appears to restrict the abilities of the local IT support administrator. I believe that this will result in a higher frequency of requests for the Help Desk. Has Help Desk support staffing and capacity been modified (increased) as a result of the FISMA requirements?

**A** The policy does restrict the abilities of the local IT support administrator to move equipment around on the 'detma.org' network and to add unspecified new equipment to the network without informing the DWD IT department in advance of the intention to do so. The goal of the new policy is to require local network administrators to be in early, close, and continued contact with the DWD IT department surrounding network configuration, local security procedures, and local IT resource administration as these activities relate to the 'detma.org' network. Additionally, the number of calls to the IT Help Desk has increased, though not by a large factor, averaging approximately five calls per day related to Network Access Control. Almost all inquiries are closed within one day. To date, Help Desk staffing has not been increased and there are no current plans to do so.

---

**Q** Has the DWD IT Dept. made any plans to assess user and customer impact of these policies (e.g. the delays in re-gaining access to equipment and services by staff and job seeker customers)?

**A** Under the policy, access violation can occur only if someone at the location in question connects something to the network or moves something on the network without notifying the DWD IT Department in advance and without making arrangements for that move or addition. To date, delays in re-gaining access to equipment and services by staff and job seeker customers have been and will continue to be the result of unauthorized or unscheduled actions of staff with regard to computer equipment connectivity to the 'detma.org' network. The protocol does not cause "unexpected' network outages.

With regard to initiating a formal user/customer impact assessment, there are no plans to conduct a formal assessment at this time. However, the need for such an assessment will be reviewed periodically.

---

**Q** To assist with planning for replacing, or moving or adding equipment, it would be useful to have step-by-step procedural guidelines for accomplishing this - including a description of the notification process.

**A** The procedure/notification process to be followed, as delineated in MassWorkforce Issuance 06-07, is to call the IT Help Desk (617-626-5555) and schedule the move and connection of equipment. The Help Desk does not have to be called if a piece of equipment is to be disconnected, but not reconnected. If however, a piece of equipment is to be disconnected and a new or replacement piece installed, the Help Desk must be called.

'Disconnecting hardware from a port with 'detma.org' connectivity without the subsequent installation of new/replacement hardware does not require a call to the Help Desk.
'Disconnecting hardware from a port with 'detma.org' connectivity with the subsequent installation of new/replacement hardware to the same port does require a call to the Help Desk.
'Moving hardware from one port with 'detma.org' connectivity to another port with 'detma.org' connectivity requires a call to the Help Desk.

---

**Q** How much advance notification to the Help Desk must be made?

**A** As soon as it is known that equipment needs to be moved or added. The more advance notice, the greater the ability to respond to the request in a timely manner.

---

**Q** Once the Help Desk is notified, how long it will take for the port for the new equipment to be activated?

**A** As stated above, the more advance notice, the greater the ability to respond to the request in a timely manner. A minimum 24 hour advance notice is recommended. While advance notice can significantly reduce the potential for delays in the final connection/activation, a specific time frame for completing the connection/activation cannot be guaranteed.

**Q** Can the CPU disconnect and the subsequent CPU re-connect be scheduled as one transaction?

**A** The protocols described in Mass Workforce Issuance 06-07 involve real-time communications protocols that result from the connection of a device to the 'detma.org' network. They are not pertinent to the physical act of disconnecting a piece of equipment from the network. These protocols involve things such as IEEE standards, CISCO system software, and NIST 800-30 et seq. While the question, as posed is not directly related to the purpose of the policy issuance, it is fair to say that if you schedule a network connection or reconnection with the IT Help Desk, it is 'scheduled'. If it isn't scheduled in advance, you are basically choosing to proceed at your own risk in terms of any issues that may arise in the process of attempting to re-connect the device without adequate advance notice. Again, as cited above, scheduling a connection/re-connection through the Help Desk in advance (a minimum of 24 hours advance notice is recommended) can significantly reduce potential delays.