2015-07

NPS Information Technology and Communications Services (ITACS) Technology News / July 2015

Monterey, California. Naval Postgraduate School
OPM to Notify Employees Re: Recent Data Breach

By now you are aware of the recent data breach of personal information from the Office of Personnel Management. However, at the time of writing this article it is still unclear exactly how many federal employees records were compromised, and how and when those employees will be notified. Despite the "churn" surrounding this breach, one thing remains clear, in today's electronic world, one must assume that their personal information is targeted 24x7 and normally there will be significant lag time between the time that their information falls into the hands of the hackers and when they are actually notified of the data breach. With that in mind, it is critical that everyone understand what they can do to protect themselves and their identity; today and everyday.

To get more information and Steps for Monitoring Your Identity and Financial Information and Precautions to Help You Avoid Becoming a Victim can all be found on the OPM website:


*Identity Theft Clearinghouse*
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.identitytheft.gov (external link)
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502

How to Connect to the NPS Campus Network Remotely

NPS users have the ability to remotely connect to the NPS network in two ways. The first and most powerful option is the Cisco VPN client. This can be downloaded and installed from either of these two sites:
https://bouncer.nps.edu or https://www.nps.edu/Technology/SoftwareLib/Auth/index.htm

Once installed on your computer, you can log into it and use your computer as though you were on campus. You will have access to all NPS resources once you are logged into the VPN Client.

The second option for remote access is through our NPS Cloudlab site: https://cloudlab.nps.edu

Once at this site, you can choose to download the client on your computer or to access it through the web browser. Log into Cloudlab, and a virtual desktop will open on your computer and you will have access to NPS resources through that virtual desktop.

Users who have used the NPS Voyager Citrix Portal (https://voyager.nps.edu) to connect remotely in the past will now have to use one of the two options above as the NPS Voyager Citrix Portal has been retired and was taken offline on June 30th.

If you have any questions or need any assistance, please contact the Technology Assistance Center (TAC).
tac@nps.edu or 831-656-1046
NPS’ Hamming Supercomputer

Did you know NPS has a supercomputer? The computer is named “Hamming”, after the internationally renowned mathematician Richard Hamming, who was a Professor of Mathematics at NPS. The supercomputer is used by faculty and students at NPS who require enormous amounts of computing power to solve a wide variety of problems. The presence of this computer on campus has also been instrumental in the recruitment of several faculty members who must have this type of equipment in order to perform their research and teaching duties.

Hamming contains 3,178 computing cores. By comparison, today a typical laptop computer might contain 4-cores. So Hamming can be thought of as having the computing power of 800 laptops tied together to solve various types of problems. Hamming also uses state-of-the-art "general purpose graphical processing units" (GPGPUs) and the specialized Intel Xeon Phi MIC co-processor to speed up certain classes of problems.

The Supercomputer is used for both classroom instruction as well as thesis research. Specialized software packages have been installed on Hamming to aid instruction and research. Several classes are taught each year using Hamming - for example: "Computer Architecture” in the Computer Science Department, "Fluid Dynamics” in the Mechanical Engineering Department, "Computer Systems” in the Electrical Engineering Department, and "Scientific Computing” in the Mathematics Department.

For more information, or to get an account, please visit www.nps.edu/hpc, or email hpc@nps.edu.

June Stats:

FY15 = 3,879 vs. FY14 = 2,791 -28%

TAC Statistics

Customer Assistance Type—TAC:
- Phone: calls made to the TAC
- Email: emails sent to the TAC for assistance
- Tech: technician dispatched to user office

To review your annual training requirements, please visit NPS’ Online Training and Certification page at (NPS Login Required):

https://www.nps.edu/technology/webbasedtraining/
The Information Technology Task Force (ITTF) provides an open forum for the review of NPS’ Information Technology strategic decision-making. The ITTF provides guidance and input to the Chief Information Officer (CIO) and Director of ITACS in the development and annual update of the NPS ITACS strategic plan.

ITTF meets on a monthly basis. A meeting was held 14 May 2015 and the main topics discussed were:

1. Cybersecurity Update
2. HPCPMO PETTT rep
3. Cloud Computing Update
4. Network Refresh
5. NHEITC Cybersecurity CONOPS

**Cybersecurity Update.** Notification commenced on 8 June regarding those affected by the OPM Data Breach. Sender of the notification **omcio@csid.com.** Please register at www.csid.com/opm with PIN provided in the email notification. Annual All-Hands Cybersecurity Training dates have been set and will be in King Hall. Dates are posted on the Security Center Wiki.

**HPCPMO PETTT rep.** High Performance Computing Modernization, User Productivity Enhancement, Technology, Transfer and Training. This service is available to those individuals who require more than what Hamming offers. The onsite rep, Jose Renteria, has a PhD in computer science and specializes in advanced computational techniques.

**Cloud Computing Update.** ITACS will initiate cloud solutions this summer. Financial, provisioning, and monitoring processes will be defined. Updates will be provided.

**Network Refresh.** The network refresh will begin this fiscal year and take a phased approach. NPS networks need to be flexible for our academic setting.

**Cloud Computing Update.** ITACS will initiate cloud solutions this summer. Financial, provisioning, and monitoring processes will be defined. Updates will be provided.

**Network Refresh.** The network refresh will begin this fiscal year and take a phased approach. NPS networks need to be flexible for our academic setting.

**Navy Higher Education Information Technology (NHEITC) Cybersecurity CONOPS** gives the NPS’ CIO, Joe LoPiccolo, authority and the local commands to orchestrate Cybersecurity to best protect data, people and networks as designated to meet mission requirements. NPS is afforded flexibility and authority to make decisions.

All meeting agendas, comments/ideas, links and presentations are posted on the Information Technology Task Force Wiki page:

https://wiki.nps.edu/x/qYCWEQ (case sensitive)

For questions contact Chris Gaucher at x 3417

---

**DISA Upgrades Web Conferencing Service**

The Defense Information Systems Agency (DISA) discontinued the Defense Connect Online (DCO) collaboration service when the DCO contract ended on June 24, 2015. DCO was replaced with Defense Collaboration Services (DCS).

Defense Collaboration Services (DCS) operate very similarly to DCO, providing users with web conferencing, multi-user chat rooms, screen-sharing, polling & voting, slide-show presentations, desktop sharing, synchronous & asynchronous meetings, and a guest feature on both the unclassified network as well as the Secret IP Data Service (formerly known as SIPRNet).

Since 2007-2008, when DCO was initially launched, it has been lauded by officials as a popular and secure communication tool despite capacity limitations. In 2013, the program grew to 800,000 users, forcing DISA to double its capacity in order to avoid poor performance during times of high demand. A big reason for the growth was DCO’s increased use for Web conferencing, as DOD sought to cut down on travel and conference expenses.

NPS users will now be able to experience higher quality Web Conferencing due to this new Defense Collaboration Services (DCS). For more information regarding this new tool please go to this link:

SAFE ~ Once Again safe for PII

The Safe Access File Exchange (SAFE) process can once again be used to transfer files with Personally Identifiable Information (PII). SAFE allows users to send up to 25 files securely to recipients within the .mil and .gov domains. The files can total up to 2GB in size. SAFE was originally designed to provide Army Missile and Research, Development and Engineering Command (AMRDEC) employees and those doing business with AMRDEC an alternate way to send files. The Department of the Navy has confirmed with AMRDEC that SAFE may be used by DON personnel to transfer files. SAFE can be accessed at the following UR: https://safe.amrdec.army.mil

Anyone (including individuals outside the Department of Defense) may use SAFE to send files to recipients with a .mil or .gov email address. However, only users with a valid DoD Common Access Card (CAC) may send files to other addresses such as .com or .edu.

NPS users also have a .mil alias for their email which can be used to receive files from non .mil or .gov email addresses: username@nps.navy.mil.

POC: Don Free, Privacyact@nps.edu

IT Scheduled Maintenance

- **Who:** NPS faculty, staff, and students utilizing the network.
- **What:** ITACS coordinates with representatives from the academic, administrative, and technical areas to plan and schedule maintenance events that affect services, which may cause services to be unavailable for up to 5 hours.
- **When:** Every Tuesday from 1730-2130.
- **Where:** Visit the NPS Intranet Home page for the latest IT maintenance announcements.
- **Unplanned Emergency:** Maintenance or special circumstances (power outages or hardware failures, for example) that require downtime are announced as necessary.

<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>1730 - 2130 Maintenance on System-Wide Network and Email</strong></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td><strong>1730 - 2130 Maintenance</strong></td>
<td>15</td>
<td><strong>16 Cybersecurity Training</strong>&lt;br&gt;King Hall 1500-1650</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td><strong>1730 - 2130 Maintenance</strong></td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td>26</td>
<td>27</td>
<td><strong>1730 - 2130 Maintenance</strong></td>
<td>29</td>
<td><strong>30 Cybersecurity Training</strong>&lt;br&gt;King Hall 1500-1650</td>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

*JULY 2015*

- **1730 - 2130**
- **Cybersecurity Training**
- **Fourth of July Holiday**