TA 13-16: Firewall Changes to Domain Name Service (DNS) Access

ATTENTION: Department of Technology Customers using DNS

ACTION REQUESTED: Notify OTech to add subnet to approved list

DUE DATE: December 30, 2013

Overview:

Currently, OTech's DNS servers support DNS resolution for any public or private entity. To minimize the possibility of OTech's DNS servers being compromised by hacking or distributed denial of service attacks, a firewall change is scheduled to take place on Sunday, January 12, 2014, at 4:00 a.m. The firewall change is a DNS best-practice required by OTech Security Management to remediate unauthorized name resolution on the internal OTech DNS servers. This change will NOT impact systems hosted at OTech.

On Thursday, December 12, 2013, OTech issued a Service Desk Bulletin regarding Change Request #54872 which identifies the subnets allowed to use DNS at OTech. That Service Desk Bulletin begins on page 2 of this Tech Alert.

Due Date:

The Requested Action below should be completed no later than Monday, December 30, 2013.

Requested Action:

Review the attached Service Desk Bulletin to identify the subnets allowed to use DNS at OTech. If your subnet is NOT listed, you are required to contact the OTech Service Desk no later than Monday, December 30, 2013, to have your department's subnet added to the access list. There may be a negative impact to your department after OTech performs the firewall change if your department's subnet is not added to the access list.

If you encounter any DNS issues after the firewall change, please contact the OTech Service Desk at (916) 464-4311 and open an Incident to have the situation remediated. Reference this Tech Alert or Change Request #54872.

Contact:

If you have questions or need further clarification, please contact your OTech Account Lead. If you are unsure who your Account Lead is, please use the Account Lead Lookup, or call the Customer Delivery Division at (916) 431-5477.

SERVICE DESK BULLETIN

Subject: Revised Date - Firewall Access Change to OTech Domain Name Service (DNS)

Reference Number:	Change Request CRQ #54872
Event Date/Time:	1/12/2014 @ 4:00 AM
Start Date/Time:	1/12/2014 @ 4:00 AM
End Date/Time:	1/12/2014 @ 7:00 AM

Summary:
The date of this firewall change is scheduled for the Network Preventative Maintenance Window on **Sunday, January 12, 2014**.

OTech internal DNS servers should only be used by OTech customers to resolve DNS queries; however, they are currently supporting DNS resolution for any public or private entity. To minimize the possibility of OTech DNS servers being compromised by hacking or by distributed denial of service attacks, a planned firewall change has been scheduled.

Action Requested:
Most OTech customers should not be affected by this change, however, **before Tuesday, December 31st**, please determine:

1. If you connect to OTech services remotely through your own Internet Service Provider (ISP) and have your PC DNS configuration directed to one or more of the OTech name servers: **ns1.net.ca.gov**, **ns2.net.ca.gov**, **ns3.net.ca.gov**, **hwu1.cahwnet.ca.gov**, or **hwu2.cahwnet.ca.gov**. If you meet both of these conditions, you will need to change your PC DNS configuration to direct DNS queries to your ISP's DNS server(s). Please contact your ISP for assistance directing your PC DNS configuration to their DNS server

2. If you have a CGEN or CSGnet connection but do not utilize one the OTech subnets listed below. If you are not certain about the subnet that you use, please contact the Service Desk and OTech staff will assist in determining your subnet and if it needs to be added to the list.

10.0.0.0/8	136.200.0.0/16	169.228.0.0/16
63.196.102.0/24	137.145.0.0/16	172.16.0.0/12
67.90.97.0/24	139.182.0.0/16	192.12.234.0/24
67.97.90.0/24	144.37.0.0/16	192.16.175.0/24
64.163.172.128/25	144.166.0.0/16	192.35.210.0/24
67.156.0.0/15	146.114.0.0/16	192.35.228.0/24
68.181.0.0/16	149.136.0.0/16	192.82.111.0/24
68.234.80.0/20	151.143.0.0/16	192.132.98.0/24
128.32.0.0/16	152.79.0.0/16	192.168.0.0/16
128.48.0.0/16	153.48.0.0/16	192.234.213.0/24
128.54.0.0/16	155.135.0.0/16	192.234.214.0/24
128.97.0.0/16	156.41.0.0/16	198.18.0.0/15
128.111.0.0/16	156.60.0.0/16	198.94.224.0/24
128.114.0.0/16	158.96.0.0/16	198.135.224.0/19
128.120.0.0/16	159.145.0.0/16	198.187.4.0/22
128.125.0.0/16	159.225.0.0/16	198.188.0.0/16
128.200.0.0/16	160.88.0.0/16	198.189.0.0/16
128.218.0.0/16	162.2.0.0/16	199.164.32.0/19
129.8.0.0/16	162.15.0.0/16	199.164.36.0/22
130.17.0.0/16	165.66.0.0/16	199.164.56.0/22
130.86.0.0/16	165.74.0.0/16	204.102.0.0/16
130.150.0.0/16	165.107.0.0/16	204.147.112.0/20
130.182.0.0/16	165.153.0.0/16	204.193.160.0/19
131.215.0.0/16	165.235.0.0/16	204.235.48.0/21
132.239.0.0/16	167.10.0.0/16	204.235.56.0/22
132.241.0.0/16	168.71.0.0/16	205.155.0.0/16
134.139.0.0/16	168.145.0.0/16	205.225.128.0/17
134.186.0.0/15	168.240.0.0/16	207.62.0.0/16
136.168.0.0/16	169.2.0.0/15	

Who is Affected:
Most OTech customers should not be affected by this change.
Customers who **may be** affected are:

1.   Those who connect to OTech services outside of a CGEN or CSGnet connection (such as through their own Internet Service Provider) and have their DNS directed to the following OTech name servers: **ns1.net.ca.gov, ns2.net.ca.gov, ns3.net.ca.gov, hwu1.cahwnet.ca.gov,** or **hwu2.cahwnet.ca.gov**

2.   Customers who have a CGEN or CSGnet connection but who do not utilize one of the above listed OTech subnets.

What to Expect:
If you are not able to resolve DNS queries (cannot access websites through the Internet) after the work is completed on **Sunday, January 12, 2014, at 7:00 a.m.,** please contact the OTech Service Desk.

An incident will be opened and OTech staff will assist you with identifying and resolving the issue.

If you have questions or comments regarding this bulletin, please contact the 24/7 Service Desk at (916) 464-4311 or Service.Desk@state.ca.gov.