

## **Remote Network Access Technology Brick V2.0**

### **Status of this Memo**

This document proposes an update to a standard for the National Institutes of Health (NIH) and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

### **Table of Contents**

1	Introduction.....	2
2	Description.....	2
3	Business Value for this Technology Standard.....	2
4	Remote Network Access Technology.....	3
5	Links .....	3
6	Summary of Comments.....	4
7	Contact.....	8
8	Changes .....	8
9	Author's Address .....	8

## 1 Introduction

This document updates the NIH Technical Architecture Standard for Remote Access Infrastructure technology for the NIH community.

## 2 Description

Remote access provides the ability for staff to connect to the NIHnet network from a distant location. This configuration requires only a computer, VPN account, VPN software, and a network connected to the Internet. The remote network could be any of the following scenarios: Non-NIH business, cable, Home, satellite, wireless modem, or tethered Blackberry networks. Remote access via a virtual private network (VPN) creates encrypted tunnels over an existing Internet connection between remote users and the network data center.

The other purpose of remote access is to enhance the wireless security offering to staff while using WLAN technologies at work. VPN over wireless adds additional security controls to WLANs while maintaining the widest possible access compatibility to staff and guests.

Security at NIH is at risk when using public network infrastructure to access NIH systems and resources. Terms like virus, malware, spam, spear-fishing, and zero-day vulnerabilities are in the news every day. Only the use of VPN and the security it employs mitigates some of the risks of the general internet. Continued use of up-to-date antivirus software, malware detection, personal firewalls, and security software updates will minimize the risks. The Security Architecture Domain Team Report provides additional guidance on applying security concepts for remote access design. The current NIH standard for VPN is Cisco Systems.

## 3 Business Value for this Technology Standard

The proven business value of this technology standard is multifaceted. On a procurement value stream, standards ensure volume pricing, and the ability to add to BPA or other rapid procurement methods. Speed of procurement reduces labor costs which reduces burden. On the compatibility value stream, standards ensure wide spread compatibility for NIH laptops and staff's home computers (where allowed). This compatibility equates to reduced labor for installation and support. This standard also equates to increased output and productivity from remote staff and contractors. This standard increases the security posture of NIH. This standard also allows for better planning for future remote access methods and applications. The multifaceted business values above all save money while increasing user satisfaction while bringing best value to the government.

## 4 Remote Network Access Technology

This brick provides baseline information of the as-is architecture (Baseline) and the future directions (Tactical and Strategic) of Remote Access Technologies as identified in this Architecture brick.

It should be noted that all technologies new to the brick are emboldened, and all technologies removed from the brick upon update are indicated with a strikethrough.

**Table 1. Remote Network Access Technology Brick**

Tactical Deployment (0-2 years)	Strategic Deployment (3-5 years)
<b>Technology</b> ■ Centralized, NIH-wide Cisco VPN	<b>Technology</b> ■ Centralized, NIH-wide Cisco VPN
Retirement Targets (Technology to eliminate)	Containment (No new deployments)
■ None	■ None
Baseline Environment (Today)	Emerging (Technology to track)
<b>Technology</b> ■ Centralized, NIH-wide Cisco VPN	■ Infrastructure as a Service
Comments	
<ul style="list-style-type: none"> <li>■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs for new products.</li> <li>■ Some baseline products have been designated as Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.</li> <li>■ Also related to encryption standards - IPsec / AES</li> <li>■ A new brick will be created to address Remote Application Access.</li> <li>■ Parachute was retired on 2008</li> </ul>	

## 5 Links

The following links are relevant to the standard at NIH.

- What is a Brick?  
<http://enterprisearchitecture.nih.gov/ArchLib/Guide/WhatIsBrick.htm>
- How to Create and Publish a Technical Standard at NIH  
<http://enterprisearchitecture.nih.gov/About/Approach/StandardsDevelopmentProcess.htm>
- Existing Remote Access Technology Brick  
<http://enterprisearchitecture.nih.gov/ArchLib/AT/TA/RemoteAccessTechnologyBrick.htm>
- VPN at NIH <http://itservicedesk.nih.gov/index.asp?Section=FAQS&Cat=15>
- VPN Tools [http://cit.nih.gov/ServiceCatalog/VPN\\_Tools.htm](http://cit.nih.gov/ServiceCatalog/VPN_Tools.htm)

## 6 Summary of Comments

### **Comment:**

Can someone help me understand "All servers and systems with remote access capabilities must reside in the NIH DMZ."? Also, does any mention or capability requirement of authentication, especially two-factor belong in this brick?

### **Response:**

Security policy covers use of login and password to all systems. This technology brick does defer to security policy when related to technology standards.

### **Comment:**

ORS recommends that we move "Remote Desktop" from Containment to Tactical Deployment until such time we can determine the impact to the NIH community. ORS Tier 2 support currently uses this solution to service client requests. Furthermore, as identified by other NIH comments, there is a need to maintain remote desktop to address potential license and use issues.

### **Response:**

The remote access Technology Brick was renamed to Remote Access Network technology Brick. An additional brick will be created called Remote application access technology brick to cover non network access. All remote access must target two factor authentications as the near future state.

**Comment:**

I believe that CIT/DECA will not be able to perform Production Support if all remote access protocols will be closed. Same will apply to Telework. We have to separate end users with Production Support/Developers. Such approach was implemented for FDCC Policies by creating AA accounts. I hope that somebody will clarify our concerns, and we will be involved in the testing.

**Response:**

The remote access Technology Brick was renamed to Remote Access Network technology Brick. An additional brick will be created called Remote application access technology brick to cover non network access. All remote access must target two factor authentications as the near future state.

**Comment:**

- We need more details on NIH- Wide VPN. What does it mean? Is it based on network (local based on NIH subnet) or software installed on our machines (VPN client with NIH certificates)? If it is based on network and we can use VPN within DMZ then why do we need VPN at all? Will they allow connecting to the NIH- Wide VPN from my home if I have my laptop with VPN client software installed on it?
- I think we need someone to weigh in here and try to define where architecture ends and policy begins.
- I will take the to-do to find someone to describe the difference between Arch (Technologies and how they fit together) and policy (how the technologies are used and the intended outcomes).

**Response:**

The remote access Technology Brick was renamed to Remote Access Network technology Brick. An additional brick will be created called Remote application access technology brick to cover non network access. All remote access must target two factor authentications as the near future state.

**Comment:**

The Table of Contents seems out of synch with the document itself.

**Response:**

Table of contents updated, thanks.

**Comment:**

- I feel that removal of Remote Desktop capability being proposed in the new brick will subject NIH to greater risk to sensitive information. It is because of Remote Desktop that I, as a NED team staff member, use to remotely log into desktop machines (after first authenticating to NIH using two-factor VPN) from non-NIH computers in order to use software that may result in access to sensitive information or needs to be configured with sensitive information in order to use. By using Remote Desktop, that software only has to be installed on government controlled computers as well as keep any information that may be accessed from being locally stored on the computer being used. The use of Remote Desktop allows the risk of any data needing to be on a locally used computer to a minimum. Also, use of Remote Desktop allows usage of a computer designated specifically for remote usage that is not necessarily located on a particular person's desk as a single point of remote access to be used by persons when needed and controlled as such. This is helpful when contractors are not given government computers to use.
- I agree. I would emphasize that this would introduce a new security risk as it would require sensitive data be stored on laptops or media that would be used at remote location (read, outside the physical network and grounds of NIH). The risk of having lost or stolen sensitive data will rise.

If we keep the Remote Desktop capability we will at least mitigate this risk since NIH maintains better control over data stored on NIH property and within its network. Once data is physically transported outside NIH property, NIH shifts security burden to user and any outside risks.

- Full disk encryption and the use of certified encrypted flash drives mitigate the risk of sensitive information being breached from a portable device.

**Response:**

The remote access Technology Brick was renamed to Remote Access Network technology Brick. An additional brick will be created called Remote application access technology brick to cover non network access. All remote access must target two factor authentications as the near future state.

**Comment:**

Please reference or comment on what "Remote Desktop" refers to. In current version of brick, there is a comment requesting "PC Anywhere" be discontinued. Yes this can be considered 3rd party remote desktop software but the most common is "Remote Desktop Connection" by Microsoft. Please confirm that this is the target for this brick so that there is no confusion.

- Agreed. If the intent is to contain any new deployments of individual solutions such as Timbuktu or PC Anywhere that should be made distinct from corporate solutions such as Citrix. Where is Citrix (or other corporate solutions) in this brick?

**Response:**

This was a relatively old brick so yes, desktop solutions version server based solutions should be differentiated.

**Comment:**

In new draft of brick there is a bullet that states...

"Due to recent NIH access policy – All servers and systems with remote access capabilities must reside in the NIH DMZ." Please give reference (or link) to this policy to facilitate discussion.

**Response:**

This was distributed to the ISSO's last month. We did not have a direct link to this policy at the time of publishing. We will update soon.

**Comment:**

Please consider moving the Remote Desktop capability from the containment category to the strategic deployment category of this brick.

When it became clear that using my personal machine to telecommute from home was a security risk to NIH, I purchased a laptop computer. Initially, we attempted to load all the software tools I needed to the laptop, but found that there were licensing issues. Of the tools that were available on the laptop, I found that processing was very slow since all data needed by the tool was moving back and forth to the NIH network over my personal line.

I discovered that I could use the Remote Desktop capability to access my desktop machine at work. I had immediate access to all the licensed software I needed and found that I worked much more quickly since Remote Desktop moves only enough data across the line to represent the updated screens.

A critical argument is that my desktop should be fully replaced by my laptop and that I bring my laptop into work to use as a desktop. My desktop is an old one but it still provides the tools I need at a speed that is effective. A cost benefit analysis could be used to show that the added cost of a desktop (or laptop) is offset by staff members being more effective while telecommuting and while generally accessing their tools remotely.

Please move Remote Desktop into the strategic deployment category of this brick.

**Response:**

The remote access Technology Brick was renamed to Remote Access Network technology Brick. An additional brick will be created called Remote application access technology brick to cover non network access. All remote access must target two factor authentications as the near future state.

## 7 Contact

To contact the NIHRFC Editor, send an email message to [EnterpriseArchitecture@mail.nih.gov](mailto:EnterpriseArchitecture@mail.nih.gov)

## 8 Changes

Version	Date	Change	Authority	Author of Change
1.1	5/24/10	Initiation		Joe Klosky
1.2	6/7/10	Minor formatting changes	NIHRFC0001	Kiley Ohlson
1.3	8/18/10	Updated based on ITMC EA Subcommittee comments	NIHRFC0001	Zahra Ashraf
1.4	8/23/10	Updated to include Summary of Comments	NIHRFC0001	Zahra Ashraf
2.0	8/24/10	Approved by the ARB	NIHRFC0001	Zahra Ashraf

## 9 Author's Address

Joe Klosky  
NIH/OCIO/ITAO  
10401 Fernwood Road, Room 3NW10B  
Bethesda, Maryland 20817-4800  
Phone: 301-496-2328  
Email: [joe.klosky@nih.gov](mailto:joe.klosky@nih.gov)