Project Charter
OLITS/OIS – Network Vulnerability Scanning
Updated April 22, 2015 - Version 1.0

<table>
<thead>
<tr>
<th>Project Name</th>
<th>UWSA network vulnerability scanning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Sponsor</td>
<td>Sasi Pillay, UW System CIO</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Nicholas Davis</td>
</tr>
<tr>
<td>Primary Stakeholder(s)</td>
<td>Tom Tenley</td>
</tr>
</tbody>
</table>

**Project Description / Statement of Work**
This project will formalize the network and IT asset vulnerability scanning and reporting of the UW System technology infrastructure by establishing a framework under which the UW System network and attached devices will be regularly evaluated for vulnerabilities and patching needs.

**Business Case / Statement of Need**
The automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened in a necessary function in the UW System computing environment.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that UW System OIS can use to tighten the network's security, improving network reliability and the protection of vital UWSA information assets.

**Customers**

<table>
<thead>
<tr>
<th>Customer</th>
<th>Customer Needs / Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom Tenley</td>
<td>Consistent, reliable, comprehensive, documented, trackable and actionable reporting of network and IT asset vulnerabilities</td>
</tr>
</tbody>
</table>

**Project Definition**

**Project Goals**
1. Evaluate the UWSA network for vulnerability scanning needs
2. Implement a scanning regimen, leveraging the network scanning capabilities of UW-Madison, such as Nessus, Qualys and other appropriate network monitoring technologies to provide regular, actionable vulnerability reporting
3. Establish a formal methodology for continuously addressing any issue identified

**Project Scope**
1. Conducting an inventory of UWSA network and attached device assets
2. Creating a list of types, frequency and targets of vulnerability scans
3. Establishing a partnership with the vulnerability scanning team at UW-Madison/DoIT to perform scans and deliver results for UWSA OIS staff
4. Anticipated scan target types include:
   - Unnecessary open shares
   - Unused user accounts
   - Unnecessary open ports
   - Rogue devices connected to the UWSA network
   - Dangerous script configurations
   - Servers allowing use of dangerous protocols
   - Incorrect permissions on important system files
### Running of unnecessary, potentially dangerous services
- Default passwords on certain devices
- Unnecessary services running on some devices
- Running web services that contain known vulnerabilities
- Dangerous applications such as peer-to-peer applications
- Third-party applications that are a vulnerability to known exploits

### Anticipated scanner types include:
- Network Scanner: General-purpose scanner that scours networks for potential vulnerabilities.
- Port Scanner: Software that is designed to search the UWSA network for open ports that attackers could use as illicit entry points.
- Web Application Security Scanner: Enables UWSA to conduct ongoing risk assessments to identify the vulnerability of web applications to hostile attacks.

### Out of Scope
1. End user owned devices, such as personal computers, tablets and mobile phones, which may attach to the UWSA network, but which are the personal property of UWSA employees

### Project Deliverables
1. An inventory of UWSA network hardware assets
2. A list of the type of vulnerabilities which will be routinely scanned for and the types of software used to perform the scanning
3. A plan for the types and frequency of vulnerability scanning and a list of devices targeted for scanning
4. A formal methodology for addressing vulnerabilities which are discovered
5. A complete documented and operationally functional network vulnerability scanning program

### Project Constraints / Risks
1. Approval of senior management to proceed with the network vulnerability scanning project is necessary
2. UW-Madison/DoIT must have the resources and time available to work with UWSA OLIT/OIS to develop and implement the vulnerability scanning program. Without such a commitment, this project will not be possible
3. UWSA OLIT/OIS staff must be willing to address the vulnerabilities which are identified, within a timely manner, in order to mitigate the potential exploitation risks.
4. Funding must be available for the required work

### Implementation Plan / Milestones
1. Meet with UW-Madison to determine what types of scanning services are available and gather the requirements for those services
2. Conduct an inventory of the UWSA network and associated hardware and software
3. Establish a priority list of hardware, and software to be scanned, types of scans, frequency of scans and determine how results will be delivered
4. Run several pilot (trial) scans on selected targets, review results, and make adjustments as necessary
5. Deploy scans in production mode across all targeted devices and systems
6. Engage in patching and other defensive activities to address issues which are identified through scans
7. Provide initial and ongoing reporting to senior management on the vulnerability state of the network, based on weekly automated vulnerability scans

### Communication Plan
1. Weekly stoplight reporting will be used to deliver current project status to senior management.
2. Email communication will be used to address small issues as they arise.
3. Informational meetings will be conducted with UWSA OLIT/OIS employees to keep them advised of the nature of the project work.

**Change Management / Issue Management**
1. Decisions will be made through advisory consultative meetings with appropriate stakeholders, and those who are working as project members and management leadership.

**Project Team Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Team members</th>
<th>Roles</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nicholas Davis</td>
<td>Project lead</td>
<td>Plan, scope, define parameters, assist technical lead as needed</td>
</tr>
<tr>
<td>Tom Tenley</td>
<td>Knowledge resource</td>
<td>Provide direction relative to resource needs</td>
</tr>
<tr>
<td>Chris Sleaford</td>
<td>Technical lead</td>
<td>Assist in the technical deployment of controls necessary to conduct vulnerability scanning</td>
</tr>
<tr>
<td>OIS technical staff</td>
<td>Patch and vulnerability management</td>
<td>Apply patches, block ports and perform other associated work to address identified vulnerabilities</td>
</tr>
</tbody>
</table>

**Stakeholder Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Roles</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sasi Pillay</td>
<td>UW System CIO</td>
<td>Managerial responsibility for all activities of OLIT and OIS</td>
</tr>
<tr>
<td>Nicholas Davis</td>
<td>UW System CISO</td>
<td>Responsible for the security program of UWSA IT assets</td>
</tr>
<tr>
<td>Tom Tenley</td>
<td>IT Manager</td>
<td>Responsible for the group which manages the UWSA network, software and associated data resources</td>
</tr>
</tbody>
</table>

**Sign-off**

**Sponsor**

____________________________________________________  Date: ____________

(Name)