

The National Association of REALTORS®
REALTOR® Secure Program

Center for REALTOR® Technology

REALTOR® Certified Security Evaluator Guide

Version 1.31

February 19, 2004



Table of Contents

Introduction	3
Levels of Certifications.....	4
National Association of REALTORS® Security Goals.....	6
National Association of REALTORS® Security Standards	7
Entity Evaluation Requirements	13
Evaluation Tasks, Tools, and Reporting Guidelines	14
Checklist.....	16
Becoming a REALTOR® Certified Security Evaluator (RCSE)	24
Certification Process Flow	25
Glossary of Terms.....	26



Introduction

The National Association of REALTORS® (NAR) has developed a security program to improve the overall security posture of its members and service providers. The program is based upon information security industry best practices.

Participation in the program can lead to an organization being certified by NAR. This distinction will lead to an organization being recognized as a security-aware organization by its customers, business partners and employees.

At the present time, there are three different types of certifications that can be obtained by various organizations:

- REALTOR® Certified Service Provider (RCSP)
- REALTOR® Certified Online Presence (RCOP)
- REALTOR® Certified Security Evaluator (RCSE)

If you are currently a REALTOR® Certified Security Evaluator (RCSE) or wish to become one, use this document as a guide. This document contains information on the various program standards, processes, and guidelines, including:

- Learn about the various Levels of Certification
- Learn about the NAR Security Standards
- Learn about the Evaluation Guidelines, Tasks, and Tools
- Apply to become a REALTOR® Certified Security Evaluator (RCSE)
- Learn how to follow the proper evaluation process to certify a Service Provider or Broker
- Learn about the terms used through out the REALTOR® Security Program.

Levels of Certifications

Participation in the program can lead to becoming certified by passing a defined security evaluation performed by a REALTOR® Certified Security Evaluator.

Participants in the program have been divided into three classifications, categorized by business role. Two of the classifications (Service Provider and Broker) are further divided by size. The entity classification and size differentiators play a strong role in the level and complexity of the participant evaluation requirements.

The three types of certifications that can be obtained by participants are:

Service Providers

Service Providers are defined as organizations providing online data services to a real estate brokerage or agent. For example: an online Multiple Listing Service for a particular area or an Application Service Provider (ASP) used to host an online presence for a brokerage or agent. Service Providers participate through the REALTOR® Certified Service Provider program.

Sizing for the REALTOR® Certified Service Provider program is defined by the number of agents serviced. These are broken down into small, medium, and large service providers and are defined as:

- Small – Less than 250 agents serviced
- Medium – 250 to 2000 agents serviced
- Large – Greater than 2,000 agents serviced

Brokers or Agents

A Broker is defined as a real estate brokerage providing buyers and sellers an online service. For example, a broker in the town of Greenville, OH has an online presence containing listings of properties for sale in the area. A buyer or seller is able to view these listings and possibly contact the broker (or one of their agents) online through online forms, e-mail, live chat, etc. Brokers participate through the REALTOR® Certified Online Presence program.

Agents who operate an online presence separate from the Broker can apply for certification separately through the REALTOR® Certified Online Presence.

Sizing for the REALTOR® Certified Online Presence program is defined by the number of agents associated with a particular broker. These are broken down in to small, medium, and large brokers and are defined as:

- Small – Less than 25 agents
- Medium – 25 to 200 agents
- Large – Greater than 200 agents

Agents use the same program qualifications as Small Brokers.

Evaluators

Evaluators are typically organizations with information security as their core competency, that have been certified by NAR as being able to accurately provide, with a high level of integrity, the security evaluation of both Service Providers and Brokers. Evaluators can participate in the REALTOR® Certified Security Evaluator program by following the participation requirements outlined in this document.

If the Evaluator is also a Service Provider, then they cannot self-evaluate.

National Association of REALTORS® Security Goals

The main goal of the REALTOR® Security Program is to raise the security awareness of the real estate industry by supplying a set of standards and guidelines to follow. As a result of the adoption of such standards and guidelines an organization will be in the position to preserve the confidentiality, integrity and availability of real estate information.

Confidentiality

The practice of sharing information only with authorized individuals and organizations.

Integrity

The practice of maintaining information that is authentic and complete.

Availability

The practice of maintaining systems used for processing, delivering, and storing real estate information so they are accessible when needed.

National Association of REALTORS® Security Standards

The REALTOR® Security Program uses the information security industry's best practices as its foundation. There are many international organizations, which have developed guidelines to help an organization increase their security posture. NAR has utilized three standards or security program models in the development of its security program. While the applicability of each model may not map completely to the real estate business, NAR has found that many of their components can be utilized to in the formation of a REALTOR® Security Program.

The security industry standards and program models researched during the development of the REALTOR® Security Program are:

(ISC)² Common Body of Knowledge

The Common Body of Knowledge [CBK] is a compilation and distillation of all security information collected internationally of relevance to Information Security [IS] professionals.

ISO/IEC 17799:2000

The ISO/IEC 17799 is the International Standard for Information Technology code of practice in Information Security. In 2000, the British Standard for Information Security (BS 7799) was adopted by ISO/IEC as ISO/IEC 17799.

VISA CISP "Digital Dozen"

The "Digital Dozen" is list of twelve basic security requirements with which all Visa payment system constituents need to comply.

The following lists of items contain the security standards that an organization should follow to participate in the REALTOR® Security Program. These should be seen as the overall security standards recommended by NAR, but some may not apply to certain Entities.

Security Policy

This refers to the documented policies that contain the fundamental principals and goals for maintaining a secure environment.

- A policy document should be approved by management and published and communicated, as appropriate, to all employees.
- The policy should state management commitment and set out the approach to managing information security.
- As a minimum, the following guidance should be included:

- a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing
- a statement of management intent, supporting the goals and principles of information security
- a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, for example:
 - Compliance with legislative and contractual requirements
 - Security education requirements
 - Prevention and detection of viruses and other malicious software
 - Business continuity management;
 - Consequences of security policy violations;
 - A definition of general and specific responsibilities for information security management, including reporting security incidents
 - References to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with

Physical Security

This refers to method of protecting against unauthorized individuals gaining access to certain physical locations containing business critical components and data within the organization.

- The security perimeter should be clearly defined.
- The perimeter of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access, e.g. control mechanisms, bars, alarms, locks etc.
- A manned reception area or other means to control physical access to the site or building should be in place. Access to sites and buildings should be restricted to authorized personnel only.
- Visitors to secure areas should be supervised or cleared and their date and time of entry and departure recorded. They should only be granted access for specific authorized purposes.
- Access to sensitive information and information processing facilities, should be controlled and restricted to authorized persons only. Authentication controls, e.g. swipe card plus PIN, should be used to authorize and validate all access. An audit trail of all access should be securely maintained.

- All personnel should be required to wear some form of visible identification and should be encouraged to challenge unescorted strangers and anyone not wearing visible identification.
- Access rights to secure areas should be regularly reviewed and updated.

Remote Access

This refers to ability for users or systems to access internal resources and information from a location outside of the physical corporate office or campus.

- Only users with a specific business requirement should be granted remote access to corporate network resources.
- User should be authenticated at the time of connection by the remote access gateway prior to being granted access to corporate network resources.
 - At a minimum authentication of remote access user should be in the form of a unique user name and password and follow the recommended password choice guidelines (see User Management).
 - Two-factor authentication can be used to mitigate the threat of passwords being guessed or shared by Entity employees (e.g. RADIUS or TACACS with tokens).
- Whenever corporate data is transmitted over public networks in conjunction with a remote access solution, encryption should be used (see Data Encryption).

Network Access Control

The ability to designate which devices within the organizations network can communicate with other internal or external devices.

- Establish a formal process for approving all external network connections (e.g. Internet, 3rd Party, or Other).
- An access control device such as a firewall should be used to separate Internet and 3rd party (business partner) networks from the Entities internal network.
- Users should be placed on separate network segments from those of the server population. This must be separated by a firewall or equivalent access control devices.
- All access control policy should be created to disallow all access through the firewall by default. Specific policy rules must be created to allow access and documented for business purpose and usage such as:
 - Outbound Internet access (e.g. HTTP, HTTPS, FTP, POP3)
 - Inbound web protocols (e.g. HTTP, HTTPS)
 - System administration protocols (e.g. SSH, SCP)
 - Other protocols required by the Entity
- Implement network address masquerading to prevent internal addresses from being translated and revealed on public networks.

- All access control policies should be audited by internal staff on a quarterly basis to identify out dated policy rules.

Intrusion Detection

This refers to ability for an organization to detect malicious activity on their systems and networks.

- An intrusion detection device should be installed and configured to examine network traffic at locations where access control devices separate Entity, 3rd party and public networks.
- The intrusion detection device should be configured to alert security personnel via manageable means in the event that unauthorized access is detected.
- The intrusion device's software and attack signatures should be updated on a regular basis.
- At an Entity where 24/7 monitoring of the device is not feasible, the Entity should consider outsourcing the monitoring responsibility to a trusted 3rd party.

Virus Protection

The methods that the organization uses to maintain the software run on systems is safe and free of malicious code (i.e., viruses).

- Detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. Protection against malicious software should be based on security awareness, appropriate system access and change management controls.
- The following controls should be implemented:
 - Install and regularly update of anti-virus detection and repair software to scan all computers and media on a routine basis.
 - Conduct regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated.
 - Check all files on electronic media of uncertain or unauthorized origin, or files received over untrusted networks, for viruses before use.
 - Check all electronic mail attachments and downloads for malicious software before use. This check should be carried out at different places, e.g. at electronic mail servers and desktop computers.

System Security

This refers to ability to maintain secure servers and workstations within an organization's environment.

- Always change the vendor-supplied defaults before a system is placed into production.
- Maintain a company standard system build for each device class in the environment. The build should take into account all known security vulnerabilities and industry best practices related to the system.
- Implement only one application or primary function per server (i.e. run the mail server on a different physical computer from the web server).
- All systems should be configured to only run necessary services.
- All systems and software should be kept up to date with the latest vendor supplied security patches.
- Install new/modified security patches within one month of release.
- Test all security patches before they are deployed to production systems.
- Implement and follow change control procedures for system software configuration.
- Implement a process to identify newly discovered security vulnerabilities.

User Management

This refers to ability to delegate authorization by individual in the access of systems and applications.

- Uniquely identify all users before allowing them to access system and network resources.
- Use at least one of the methods below to authenticate all internal and external users:
 - Unique username and password
 - 2-factor (e.g. tokens or certificates)
 - Biometrics
- Ensure proper password management by:
 - Controlling the addition, deletion, and modification of user IDs.
 - Immediately revoke access of terminated employees
 - Distributing password policies, procedures and guidelines to all users on a regular basis
 - Not permitting group passwords
 - Changing user passwords every 90 days.
 - Requiring a minimum password length of at least 7 characters.
 - Should not be found in a dictionary of commonly used words.
 - Using passwords that contain both at least 1 number and 1 symbol (e.g. !,@,#, or %)
 - Monitoring access attempts.
 - Locking out users after 6 failed authentication attempts.

Data Encryption

This refers methods of storing and transmitting data using cryptographic technology to maintain confidentiality and integrity.

- Implement a cryptographic solution that:
 - Is isolated so that secret data cannot be disclosed
 - Conforms to applicable international and national standards
- Protect encryption keys against both disclosure and misuse by:
 - Restricting access to the encryption key to the fewest number of individuals
 - Store encryption keys securely in the fewest possible locations
- Fully document all key management processes and procedures.
- All Entity originated data that is transmitted over public networks should be encrypted so that it can only be decrypted by its intended recipient (e.g. SSL and IPsec).
- Data classified as business confidential that is transmitted over Entity networks, should be encrypted so that it can only be decrypted by its intended recipient.
- Data classified as business confidential should always be stored (when possible) in an encrypted form, so that it can only be accessed by systems or individuals specifically requiring such access.

Disaster Recovery

The organization's documented process for ensuring the acceptable availability of their environment for the online services they are providing.

- Backups of systems containing business critical data (i.e. financial data, employee records, client records) should be made on a daily basis.
- At least one back up per week should be stored at an offsite data storage facility.
- Restoring systems and data from backups should be tested on a regular basis.
- All systems or data connections providing critical business functions should be made highly available, e.g. application and database servers, data carriers, firewalls and authentication systems

Entity Evaluation Requirements

In the table below, Entity types has been mapped to an evaluation requirement. Also, the estimated effort by the Evaluator and cost to the Entity has been identified. These costs do not include estimated travel and expenses incurred by an Evaluator while performing on-site evaluation tasks.

Exhibit 4: REALTOR® Security Program Entity Evaluation Requirements

Certification	Size	Evaluation Requirement	Estimated Effort	Estimated Cost to Entity
REALTOR® Certified Service Provider	Small	Questionnaire Phone Checklist Remote Scan Policy Review	8 – 16 hours	\$1200.00 – 2,500.00
	Medium	Questionnaire Phone Checklist Remote Scan Documentation Review	24 – 40 hours	\$3,600.00 – 6,000.00
	Large	Questionnaire Face-to-Face Interviews Remote Scan Documentation Review Device Configuration Review Internal Scan	60 – 100 hours	\$9,000.00 – 15,000.00
REALTOR® Certified Online Presence	Small	Questionnaire Phone Checklist Remote Scan	3 – 10 hours	\$500.00 – 2,000.00
	Medium	Questionnaire Phone Checklist Remote Scan Documentation Review	12 – 20 hours	\$2,000.00 – 4,000.00
	Large	Questionnaire Face-to-Face Interviews Remote Scan Documentation Review	36 – 60 hours	\$5,000.00 – 10,000.00

Evaluation Tasks, Tools, and Reporting Guidelines

This section contains the items used during an evaluation. Over the life of the security program, modifications may be made. The most recent version of this document will always be found on the website.

As an Evaluator, you must follow all guidelines presented below. Failure to present a report that follows NAR guidelines will result in your organization no longer being allowed to perform these evaluations as part of the REALTOR® Security Program.

Questionnaire

The questionnaire below has been developed to serve as a pre-evaluation data gathering tools. This questionnaire can be reformatted or placed on a website to gather this information on-line, given that the data is transmitted over SSL. As an Evaluator this information is important to gather prior to beginning any of the other evaluation tasks, since much of the information gathered here will prepare you for the tasks ahead.

Exhibit 1: REALTOR® Security Program Questionnaire

Name:
Title:
Company:
Email Address:
Phone Number:
Fax Number:
Address:
City:
State:
Zip Code:
1. Do you own a website? Yes or No
2. If so, what is the URL?
3. Describe the purpose of your website?
4. Do you receive client information via the website? Yes or NO
5. Is the website hosted at your office or is it outsourced to a service provide?
6. If you use a service provider, please provide the name and contact info service provider.
7. May we contact your service provider on your behalf?

8. How many office locations do you have?
9. How many employees per location?
10. How many if these are agents?
11. If you are a Service Provider, how many agents do you serve?
12. Does each office have an Internet connection? Yes or NO
13. If you host your own website, what other public IP addresses do you own?
14. Which of the following items do you have or operate in your environment? (For each please specify the vendor of origin)
 - o Corporate Security Policy
 - o Mail Server
 - o Router
 - o Switch
 - o FTP Server
 - o DNS Server
 - o File Server
 - o Database Server
 - o Web Server
 - o Application Server
 - o Firewall
 - o Intrusion Detection System
 - o Gateway Virus Server
 - o Desktop Virus Scanner
 - o Vulnerability Scanner
 - o VPN Gateway
 - o Remote Access Gateway (Dial-up Server)
 - o 2 Factor Authentication System
 - o Public Key Infrastructure (PKI)
15. Have you ever participated in a security assessment, penetration test, vulnerability scan or all of the above?
16. If so, when was the last time you had one performed?
17. When is the best time of day to perform a remote security scan of your environment?
18. What concerns do you have about this evaluation process

Checklist

A security checklist has been developed for the REALTOR® Security Program. The checklist covers questions pertaining to each of the REALTOR® Security Standards. The table below should be used during the interviews of the Service Provider or Broker key contacts.

Reading the table from left to right, the REALTOR® Security Program “Category” is identified.

The next column is “Code”. Since there are many different size organizations that may be evaluator during the REALTOR® Security Program, NAR has decided upon which standards will apply to each of the different Entity types. These codes should not be shared with Entity being evaluated. The following is a list of each of the possible codes:

- **ALL** – The standard is applicable to all Entities.
- **OPT** – The standard is optional to all Entities at this time. Each optional should still be documented like the other standards for future reference by NAR, but the “Compliant” field should not be filled in.
- **SP** – The standard is applicable to all Service Providers. The code of **SP + S, M, or L** states that the standard is applicable to Small, Medium, or Large Service providers.
- **BR** – The standard is applicable to all Brokers. The code of **BR + S, M, or L** states that the standard is applicable to Small, Medium, or Large Brokers.

The next column is the “NAR Security Standard” that the Service Provider or Broker should be evaluated against.

The next column titled “In Place” should be filled out for each standard. This should contain a detailed description of what the Service Provider or Broker has in place in their environment. This may be just a restatement of the standard or a statement showing a slight difference from the standards.

In the “Compliant” column, a Yes or No answer should be given. For each “No” item in the checklist one of two responses are required:

- Not Applicable – The Evaluator must supply justification for the item being not applicable to the organization's environment.
- Not Compliant – The Evaluator must supply the anticipated date of compliance as provided by the organization.

Exhibit 2: REALTOR® Security Program Checklist

Category	Code	NAR Security Standard	In Place	Compliant
<i>Security Policy</i>	ALL	The security policy exists within the organization.		



	ALL	The security policy was approved by management.		
	ALL	The security policy is published and communicated to all employees.		
	ALL	The security policy states management's commitment to security.		
	ALL	The security policy discusses the organization's approach to managing information security.		
	ALL	The security policy contains a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing.		
	ALL	The security policy contains a statement of management intent and supports the goals and principle of information security.		
	ALL	The security policy contains a brief explanation of each of the security policies, principles, standards, and compliance requirements of particular importance to the organization.		
<i>Physical Security</i>	ALL	The security perimeter is clearly defined.		
		The perimeter of the building(s) containing information processing facilities is physically sound and contains:		
	ALL	1. no gaps in the perimeter or areas where a break-in could easily occur		
	ALL	2. walls of solid construction		
	ALL	3. external doors that are suitably protected against unauthorized access		
	SP BR+L	4. a manned reception area		
	ALL	5. a visitor log to restricted areas		
	SP	6. access badges or proximity cards for access to restricted area		
	SP	7. personnel wearing visible identification		
	ALL	Access rights to secure areas are regularly reviewed and updated.		
<i>Remote Access</i>	ALL	Users with a specific business requirement are granted remote access capabilities.		
	ALL	Users are authenticated prior to accessing corporate network resources.		
	ALL	Authentication is in the form of a unique username and password.		
	ALL	Data encryption is used when corporate data is accessed over public networks.		



<i>Network Access Control</i>	ALL	There exists a formal process for approving all external network connections (physical or virtual circuits), including documentation referencing the business case for each connection.		
	ALL	An access control device such as a firewall is used to separate public, 3 rd party, and corporate networks.		
	SP+ML	Users are located on separate network segments from those containing servers.		
	SP+ML	Users segments are separated from server segments by a firewall or equivalent access control device.		
	ALL	All access control policies applied to network access control devices are created to disallow all access by default.		
	OPT	Network address masquerading is used to prevent internal (corporate) addresses from being translated and revealed on public networks.		
	ALL	Access control policies are audited by internal staff to identify out dated policy rules.		
<i>Intrusion Detection</i>	SP+L	Where network access control devices separate trusted from untrusted networks an intrusion detection device is installed and operational.		
	SP+L	The intrusion detection device alerts security personal in the event that unauthorized access is detected.		
	SP+L	The intrusion detection device is frequently updated from a software and attack signature standpoint.		
	SP+L	The intrusion detection device is monitored on a 24/7 basis.		
<i>Virus Protection</i>	ALL	Users are educated on detection and prevention of viruses.		
	ALL	All computers have anti-virus software installed.		
	SP BR+L	Regular reviews of the software and data content of systems supporting critical business processes is conducted.		
	ALL	All files on electronic media of uncertain or unauthorized origin are checked for viruses before use.		
	ALL	All electronic mail attachments and downloads for malicious software before use.		
		Virus checks are performed at the following locations:		
	OPT	1. Gateway		
	OPT	2. Mail Servers		
	ALL	3. Desktops		
<i>System Security</i>	ALL	Vendor-supplied defaults are changed before a system is placed into production.		



	SP+ML BR+L	Standard builds for each system class exist.		
	ALL	Server builds take into account all known security vulnerabilities and industry best practices.		
	OPT	Only one application or primary function per server in production.		
	ALL	Systems are configured to only run necessary services.		
	ALL	Vendor supplied security patches are installed within one month of release.		
	SP+ML	All security patches are tested before they are deployed to production systems.		
	SP+ML	Change control procedures are followed for system configuration modification.		
	ALL	A process exists to identify newly discovered security vulnerabilities applicable to the corporate environment.		
<i>User Management</i>	ALL	All users are uniquely identified before being granted access system and network resources.		
		One of the following methods are used to authenticate internal and external users:		
	ALL	1. Unique username and password		
	OPT	2. 2-factor (e.g. tokens or certificates)		
	OPT	3. Biometrics		
		Confirm that password management:		
	ALL	Controls the addition, deletion, and modification of user IDs		
	ALL	Immediately revokes access of terminated users		
	ALL	Distributes password policies, procedures and guidelines to users		
	ALL	Does not permit group passwords		
	ALL	Requires the changing of user passwords ever 90 days		
	ALL	Requires the minimum length of at least 7 characters		
	ALL	Passwords cannot be found in any commonly used dictionary		
	ALL	Requires password choice to contain at least 1 number and 1 symbol		
	ALL	Monitors access attempts		
	ALL	Locks out users after 6 failed authentication attempts		
<i>Data Encryption</i>	ALL	A cryptographic solution exists that:		
	ALL	Is isolated so that secret data is not disclosed		
	ALL	Conforms to applicable international and national standards		
	ALL	Encryption keys are protected against both disclosure and misuse by		



		only allowing access to keys by the fewest number of individuals and storing keys securely in the fewest possible locations		
	ALL	All key management processes and procedures are fully documented.		
	ALL	Confidential data that is transmitted over public networks is done so in a manner that can only be decrypted by the intended recipient.		
	OPT	Confidential data is always stored in an encrypted form.		
<i>Disaster Recovery</i>	ALL	Backups of data on business critical systems are made daily.		
	SP BR+L	At least one backup per week is stored at an offsite storage facility.		
	ALL	Restoration tests of backed up data are performed on a regular basis.		
		Components of the environment providing critical business functions are highly available. These include:		
	OPT	Data connections		
	OPT	Firewalls		
	OPT	Servers (Database, Application, Web, Mail, DNS, Authentication Servers, etc.)		



Face-to-Face Interviews

An interview consisting of a walk through of the above checklist should take place. The interviews should be limited to 4 individuals within the organization. The conversation should be limited to 1 hour.

Individuals requiring separate face-to-face interview can include:

- IT Director
- Security Manager
- Network Administrator
- System Administrator
- Database Administrator
- Application Developer

The interviews should contain a walk through of the same checklist with each individual, to reveal any inconsistencies that may exist.

Remote Security Scans

A remote scan will utilize open source tools to evaluate network and system configurations as seen from the Internet. In addition, the tools will be used to identify any vulnerability present within network and system devices.

The standard tools are:

- Nmap – A tool used for network mapping and Operation System identification. This tool will be run first of the external environment. The output will be documented and used as input for the Nessus scan.
- Nessus – A vulnerability assessment tool, frequently updated by the security community with the latest vulnerability checks. This tool will be run against the Internet accessible environment.

No Denial of Service (DoS) scans will be run by the Evaluator.

All Entities are required to undergo a Remote Scan of their environment as part of the evaluation.

Documentation Review

The Evaluator will gather documented diagrams depicting the configuration and organization of device on the Entities network. The Evaluator will examine these diagrams for security industry best practices and make recommendations for improvement.

Policy Documents

Up to 4 policies will be collected and reviewed for completeness. These can include but are not limited to:

- Acceptable Use Policy
- Anti-Virus Process
- Remote Access Policy
- Router Security Policy
- Password Protection Policy
- Server Security Policy

Device Configuration Review

Up to 3 critical devices within the environment will be reviewed this can include but are not limited to:

- Firewalls
- Web Servers
- Database Servers
- Routers
- Intrusion Detection Systems

Internal Scan

An internal scan will utilize open source tools to evaluate network and system configurations as seen from the internal network. In addition, the tools will be used to identify any vulnerability present within network and system devices.

The standard tools are:

- Nmap – A tool used for network mapping and Operation System identification. This tool will be run first of environment. The output will be documented and used as input for the Nessus scan.
- Nessus – A vulnerability assessment tool, frequently updated by the security community with the latest vulnerability checks. This tool will be run against the internal environment.

No Denial of Service (DoS) scans will be run by the Evaluator.

Report Guidelines

The report must be securely distributed to NAR and Entity by the Evaluator. The report must be saved in Rich Text Format (RTF) or plain text format before it is distributed to NAR and Entity by the Evaluator. The Evaluator must apply the following content and format when completing the report:

- Executive Summary
 - Include the following:
 - Describe the nature of the Entity's business.
 - Classify the Entity (i.e. Small Service Provider)
 - Describe the environment in which the evaluation was focused (i.e. Entity's Internet access points, internal network)
 - A statement stating recommendation for or against certification:
 - Yes
 - Yes, after some changes (list changes)
 - No
- Scope of Work and Approach
 - Describe the depth to which the evaluation was performed and a high-level overview of the methodology
 - Timeframe of the evaluation (i.e. when where the tasks performed?)
- Findings and Observations
 - Document the results of each of the evaluation tasks performed
 - Provide recommendations for remediation of any non-compliant items
- Contact Information and Report Date
 - Entity Contact Information
 - Evaluator Contact Information

Becoming a REALTOR® Certified Security Evaluator (RCSE)

In order to become a REALTOR® Certified Security Evaluator (RCSE) the follow rules and tasks must be followed:

- All applicants should have information security as their core competency
- Review and understand this document in its entirety.
- Be able to accurately provide, with a high level of integrity, the security evaluation of both Services Providers and Brokers.
- Email to the following information to info@crt.realtors.org, with a subject of "Evaluator Application".

The REALTOR® Secure application is located on the REALTOR® Secure website at:

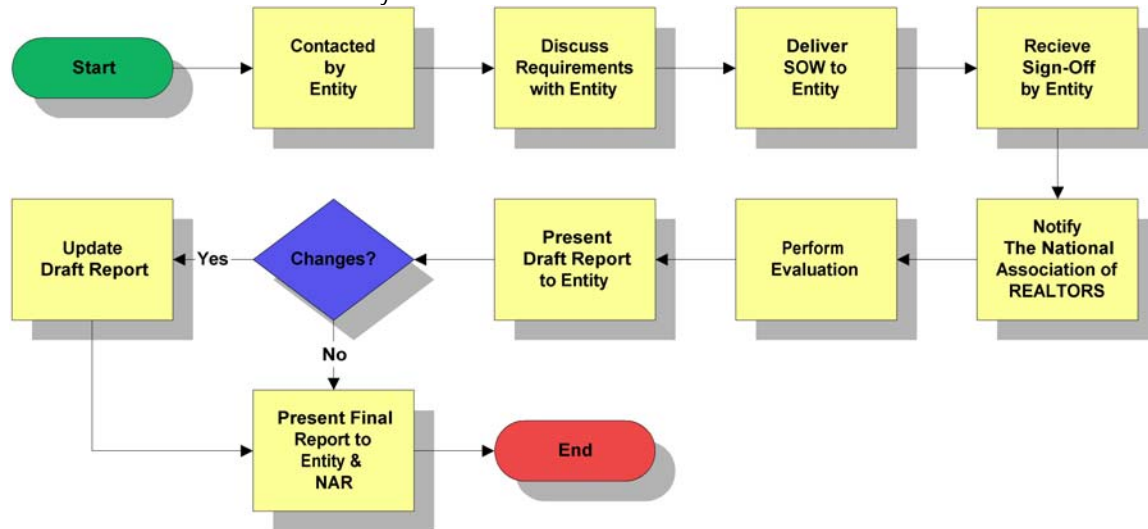
<http://www.realtor.org/secure>

the application requests contact information about the evaluating organization, security concentrations and other information needed to ensure a successful partnership.

- If the application is accepted by NAR, then the Evaluator will be lists as REALTOR® Certified Security Evaluator on the website.
- The Evaluator must submit an updated application each year to maintain their status as a REALTOR® Certified Security Evaluator.
- NAR reserves the right to terminate any Evaluator relationship at any time and for any reason.

Certification Process Flow

Exhibit 5: REALTOR® Certified Security Evaluator Process Flow



1. Evaluator is contacted by an Entity to perform a security evaluation.
2. Evaluator discusses the evaluations requirements with the Entity.
3. Evaluator provides Entity with a Statement of Work (SOW) with the description the evaluation tasks to be performed and the estimated costs.
4. Evaluator receives a signed SOW from the Entity with the appropriate payment arrangements.
5. Evaluator contacts NAR to inform that an evaluation is set to begin for a particular Entity.
6. Evaluator performs the evaluation based upon the predefined evaluation requirements.
7. One week after the evaluation, the Evaluator sends the draft report from the Entity. The Evaluator gives the Entity one week to respond or dispute any of the findings described within the report.
8. Evaluator sends the final report to NAR and to the Entity in the form outlined in the "Report Guidelines" section of this document.

Glossary of Terms

Attack Signatures – The network traffic patterns used by IDS (see Intrusion Detection Systems) to detect a potential hacking attempt.

Audit Trail – The chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

Biometrics -- A method of generating authentication information for a person by digitizing measurements of a physical characteristic, such as a fingerprint, a hand shape, a retina pattern, a speech pattern (voiceprint), or handwriting.

Business Continuity Management – The combined emergency response, backup operations, and post-disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis.

Certificate – A digital data document assigned to object (system or individual) used to authenticate the object during a transaction (system or network access, data exchange, etc.)

DNS – An acronym for Domain Name System. The main Internet operations database, which is distributed over a collection of servers and used by client software for purposes such as translating a domain name-style host name into an IP address (e.g., "www.realtor.org" is "32.97.215.193") and locating a host that accepts mail for some mailbox address.

Encryption Key -- A cryptographic key that is used to encipher application data.

Firewall -- An internet-work gateway that restricts data communication traffic to and from one of the connected networks and thus protects that network's system resources against threats from the other network.

High Availability -- The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.

Information Security Industry Best Practices – a collection of internationally accepted processes and technologies used by organizations to secure data processing environments.

Intrusion Detection System – A security service that monitors and analyzes system events for the purpose of finding and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Malicious Activity – An action performed by an individual, virus or worm intentionally harming a system, network, application or data.

Network Address Masquerading – A network where packets traveling to and from the internal network are translated for private addresses, so they are not revealed to the public.

Remote Access Gateway – A device that user or devices dial into using a modem in order to gain access to resources on the network the device is attached.

Secure Areas – A location in a building where only authorized individual should be allowed to enter.

Security Patches – A code update intended to resolve a security issues within one or more of the components an operating system or software package.

Security Posture – The overall view of an organization from a security stand point.

Tokens – A device used by an authentication system to supply one time unique passwords.

Two-factor Authentication – A higher level of authentication than a unique user name and password. Something that a user has (a certificate or token) above something that the user knows (a password) makes up the second factor of authentication.

Portions of the Glossary of Terms were obtained from IETF RFC2828
<<http://www.ietf.org/rfc/rfc2828.txt>>