A WHITE PAPER FOR:

Portable Systems Devices

Category Type: Operational Systems Security and Architecture

Topic 1: Secure Virtual Portable Systems Device

PREPARED FOR:

General Release

BY:

Sky Catcher Solutions
P.O Box 183
Rutherfordton, NC 28139

March 2011

Electronic Submission

Section 1 — Executive Summary

This paper briefly describes a concept of developing and integrating a technology to allow users and organizations to deploy a highly secure mobile virtual computing platform throughout their own personal computers or even throughout an Enterprise deployment. Throughout this paper this idea will be described as a Portable Systems Device or PSD.

The applicability to the end user and ultimately, to an entire Enterprise to this technology is multifaceted. Enterprise organizations all over the world have long asked for a solution that will meet not only their Data-at-rest (DAR) requirements, but also provide for a computing platform that is properly secured and enterprise manageable. This virtualized computing platform should not be vulnerable to data contamination from the host on which it resides no matter whether that host sits inside a protected enclave or at residence of a teleworker. It should also be ultra portable to facilitate the movement of the device from one location to another without the need for re-registration or reconfiguration. Data-in-transit is also a key area of concern. Data on sensitive networks should be protected while it is in motion and data should be able to traverse the Internet when personnel are not directly connected to or through their Enterprise).

The core of our approach is to create a product unlike any other available on the open marketplace. The proposed technologies create a virtual computing platform that provides strong authentication, is FIPS 140-2 encrypted, meets even stringent Department of Defense standards , is truly portable, and leaves zero residual footprint on the physical host which it was connected. The solution also should be readily enterprise manageable not only to the PSD platform, but to security controls put into place by Security Administrators within the Enterprise . The technology is ready for any environment and deployment now. This paper defines the capabilities brought by this technology. It will also define different options to implement this solution and discuss the strengths and weaknesses of each of those options.

The technologies described in this white paper will be as follows:

i. Secure Portable Systems Device Types
ii. Secure Virtual Private Network Tunnel Capabilities
iii. Enterprise Management Capabilities
iv. Uses as a secure storage ONLY (if desired)
v. Biomedical applications and other anticipated usages

The paper will further discuss this PSD implementation including:

Section 1: Conceptual Ideas and Components
Section 2: Solution Types, Scope and Options Available
Section 3: PSD Device Configuration Types
Section 4: Use Case Studies
Section 5: Conclusion
Section 6: Contact Information

Section 2 — Conceptual Ideas and Components

The proposed technical approach to virtualizing and securing these computing platforms is multifaceted. It must be user friendly and intuitive while at the same time maintaining ALL security requirements. All technologies bring with them new challenges not only to the end user but also to the System Integrator/Maintainers as well. The first technical hurdle to overcome is to offer an interface that is not only familiar to the user, but also secure from the onset and that fits into the security framework that has already been established by the Enterprise and is manageable by current systems maintainers. Introduction of this virtual computing platform will present a familiar environment to all users and Systems Administrators (SA) allowing them to immediately benefit from its integration. There will be no learning curve or ramp up time on its use. The computing platform can however, be tailored to almost any Operating System and to almost any configuration. One of the most important aspects of the computing platform is that it must meet all customer, security and operational requirements. When the solution is implemented, it should not affect current implemented programs or user experience at all.

Technical hurdle two is to adhere to Information Assurance specifications while maintaining usability and familiarity to the end user and administrators and to alleviate the need for training of new systems or components. Following requirements from Department of Defense and Federal guidelines as well as other IA requisites, this Portable System Device solution is fully security compliant to any scenario it is introduced to, including the Department of Defense. This solution, however adopted, is also secure when it is not in use at all. The data on this virtual platform is secured by an onboard hardware encryption processor which provides strong AES-256 bit encryption. The encryption standards are already certified to the FIPS 140-2 standard. If a device is lost or stolen, there is no chance of the data inside being compromised. Aside from the strong encryption, the solution has enterprise management capabilities that allow both Security and Systems Administrators to perform their jobs effectively from solution initiation without the need for additional training. On a network, the devices function just as any other host computer would act on a network. Maintenance of the devices themselves is accomplished from the device enterprise management console. Device enterprise management offers roles based administration and the ability to perform a variety of functions from resetting a password to remotely wiping a device if it is lost or stolen. This offering is a computing platform that from its adoption by the Navy is secure, IA compliant, and enterprise manageable.

Even as the solution is FIPS compliant with strong encryption and the data is secured onboard the device, authentication into the device must be just as effective and easy to accomplish. The design of the device is such so that it is capable of two factor authentication. Devices that have smart card (CAC/PIV) and password provide the highest degree of assurance and authentication. This truly enforces the “What you have, what you know, and what you are” rule of authentication. Technical hurdle three is solved with up to two factors of

authentication ensuring that the person accessing the device is in fact, an authorized user.

The fourth technical hurdle that has to be overcome is the challenge of securing the communication channel even when a user is not in his native AOR (IE: Not directly connected to the Enterprise network or when being used as a teleworker device). Since protection of data-in-transit is a major security concern within any organization, the creation of a unique VPN tunnel that will transport the identity of the virtual computing platform to anywhere desired. It also will conceal and secure the transmission of data within that tunnel in a FIPS approved security architecture. Since the client is based on the OpenVPN platform it is highly customizable and can be tailored to the unique situation within the architecture it is placed. Additionally, and equally as important, since the security of the servers that create the tunnel need to be within the protected enclave, the tunnel itself can be virtualized and placed wherever there is a need and is available now. The client can be integrated into the PSD as part of the default configuration with organizational security certificates included.

2.1 Scope

The scope of the proposed solution is to –

- Present a ultra mobile “go anywhere” platform that can travel with a user into any situation in which they are placed
- Secure this platform with FIPS certified encryption modules
- Have up to three factor authentication if required
- Provide a secure communication tunnel no matter where the user is connected and performing device anonymization and obfuscation.
- Maintain all IA standard and remain IA compliant as delivered to the Enterprise and maintain that compliance throughout its lifecycle
- Facilitate a paradigm shift in which a virtual computing device is issued as part of an employment process or as an alternative to extremely vulnerable home computers. This computing device is capable of holding authentication credentials, network access controls, biomedical data, and much more while staying with a user as long as they carries the device.

2.2 Conceptual Architecture

The baseline for this concept is simple; computing platforms that will facilitate thin client type access and allow secure portability and protected communications. There are basically two different scenarios on how this solution could be deployed. Both have similar enterprise management; offer enhanced encryption and a VPN to protect data in transit. Both will be discussed in the following paragraphs.

2.2.1 Microsoft Windows VM Architecture

This architecture is basically the use of a portable USB device that boots from a Microsoft Windows preboot environment on a host computer into a preboot authentication application. After successful authentication, the device reboots the host computer and arrives in a native Microsoft Windows VM Operating System. This VM environment is almost identical in nature to Microsoft Windows XP Professional. This scenario solves the familiarity problem by presenting the user with a familiar interface and it offers driver support for over 12,000 devices. The Operating System if configured correctly, will not allow access to the underlying host hardware. This nearly eliminates the chance of contamination from the underlying host computer. In addition, Windows VM (SCS) devices offer enhanced write filters to help prevent users from becoming infected Internet-borne threats or from them installing unauthorized software of any kind. The Operating System can have multiple standard configurations keeping in mind that hardware support may be limited due to the need for separation of the physical host components. In other words, if a driver is loaded that offers access to the physical host hard drive, there is a chance of potential contamination from that drive, if a driver to the physical host is not loaded, then there is very little chance. In all, hardware configuration on a SCS device can be extremely difficult and difficult to configure. Software can be loaded and run as in a normal computer and documents can be stored on the device itself or shared across a network connection to a cloud. Virtual devices such as CD-ROM libraries are difficult to load and maintain because of the lack of support for virtual device drivers. If new software or security updates are required, the device is launched in a “maintenance” mode which allows new software updates to persist across reboots. If an OS becomes corrupted, the device can be reimaged with its base image again providing for minimal downtime. Administratively, the SCS solution provides for the same administrative functions offered in a physical host running Windows XP, from a network management standpoint there is no difference between the two. The only real role for SCS is teleworkers. It is not readily capable of a variety of other roles such as forensic platform or first responder device.

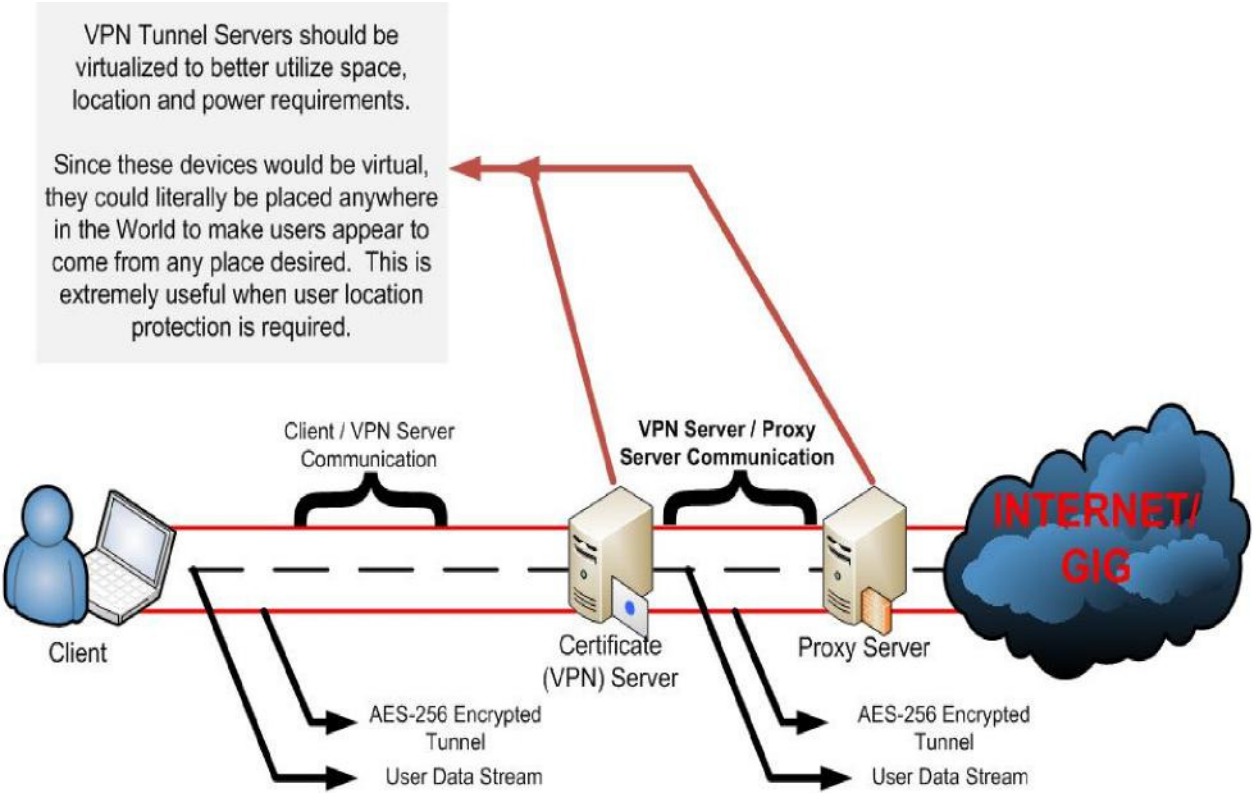
2.2.2 Linux Boot Running Virtual Operating System

The other type of configuration available would be to have a Linux booting Operating System. In this configuration, a portable USB device that boots from a Linux (usually Ubuntu) preboot environment on a host computer into an authentication application. After successful authentication, the device launches VMWare player and then a virtualized host operating system. That Operating System can be just about any OS from Windows XP to Linux. The only consideration would be the minimum required hardware to run an OS. For example, running Windows Server 2008 from the device would be ineffective unless the physical machine were capable of running Windows Server 2008. Generally speaking, Windows XP and most Linux variants are safe to run on almost any hardware found in any environment. Since driver and kernel support is provided by the underlying Linux OS, nearly all of the hardware available on the open market is accessible to the Virtual OS. Security is enhanced greatly by running a Linux Boot device as well. Not only is the base Linux image secured to DOD standards, but the Virtualized OS can be tightly configured and secured to DOD IA directives as well. Hardware can be managed by the underlying Linux

OS AND the VMWare image to restrict access to any or all of the physical host. This means that this solution can take on multiple roles such as a forensics platform or first responder device. If image corruption occurs, the feature of VMWare to “step back in time” to an earlier snapshot of the OS will all but alleviate downtime. Software can be run and loaded by users and documents can be saved to the device or to the cloud. This can be controlled by Information Assurance management components. Virtual devices can be loaded and maintained easily. In addition, software write filters can be engaged in a VMWare host to disallow writing to critical system files, especially in a guest Windows OS.

2.2.3 Conceptual Architecture

The figures below show basic block level conceptual architecture for both the Portable Systems Environment (PSD) in either the SCS configuration or Linux Boot configuration environment as well as the VPN:



Generally speaking configuration of any of the possible solutions is architecturally the same. The difference lies in how the underlying OS interacts with the physical host. The following section will explore cost, configuration, and maintenance of each of the possible solutions.

Figure 2.2 – VPN Conceptual Block Diagram and Functional Layout

Section 3 — PSD Device Configuration Types

Since there are multiple configurations, cost savings can vary from a slight savings on current technology to a significant cost savings depending on which platform is chosen. It is notable that a Windows VM solution has already gained Department of Defense acceptance. A Linux booting solution running a Microsoft Windows Virtual Machine is nearly identical in security function, but generally more customizable and offers a better security platform to work from. The following section will analyze the benefits and weaknesses of the two basic kinds of configuration for a PSD.

The following capabilities/feature table shows the device features. Immediately following the table, each of the features will be explained in detail.

Feature	Capability
16 / 32 / 64 GB sizes	X
Preboot Authentication	X
Choice of Operating System	X
Customizable Virtual OS	X
	X
Robust Security	X
FIPS 140-2 (3) 2011	X
DISA STIG	X
Common Criteria 2011	X
CAC Enabled	X
Master Password	X
User Password	X
Role based permission	X
Wipe device data	X
Tamper Resistance	X
Security Administration	X
	X
Device Role Customization	X
Enterprise Manageable	X
Support for multiple administrators	X
System wide policies	X
Reset to default configuration	X
Network / remote management	X
Update Device version	X
White list / Blacklist	X
Disable device	X
Remote Disable / Delete	X
Password Management	X
Remote Management	X
Offline Restrictions	X
Audit and Reporting	X
Advance Filtering	X
Message / Email Alerts	X

3.1 Feature Table Breakdown

3.1.1 **Preboot Authentication –** In either scenario described preboot authentication is easily accomplished. The preboot environment launches an authentication program that users will authenticate to the level set by the Systems Administrator. This authentication can be up to 3 factor authentication. Upon successful authentication, the preboot environment will execute the user boot environment and the user will be placed into the OS running on the device.

3.1.2 Choice of Operating System – SCS devices boot natively into a Windows Preboot (WinPE) environment and after authentication boot into Windows VM Standard. There is no other option other than that. Linux boot with virtual guests offer the ability to choose almost any Operating System to boot into. As long as the physical host the device is placed into can accommodate the device duty, the OS will work.

3.1.3 **Customizable Virtual OS –** The Windows and Linux VM Operating Systems can be customized and a "golden image" created. Users can load software based on their administrative rights on the network. This matches how a typical physical computer would work.

3.1.4 **Robust Security –** SCS devices offers an additional single layer of protection. The write filters that are enabled prevent users from writing to or changing system files or folders. This is effective and offers adequate protection from malicious insiders. With a Linux device and a Virtual Host, administrators are offered more choices and a greater protection profile. This scenario almost completely prevents even a skilled, but malicious insider from tampering with the device and making unauthorized changes.

3.1.5 Security Administration – Security is nearly identical on each of the two platforms. Security Updates and patches are applied exactly as they are today and the Enterprise programs that manage them can be used to do that task.

3.1.6 Enterprise Manageable – Both solutions offer an enterprise management capability. Both have management capabilities that offer the ability to remotely administer the device. Passwords can be reset if forgotten, devices can be remotely administered, and user maintenance can be performed.

3.1.7 Device Role Customization – The SCS devices are best suited for teleworker application. They offer little capability other than that role because of the inability to interact with the underlying kernel. However, Linux boot devices offer almost countless possibilities when choosing what role the device will perform. Linux devices can be configured as biomedical devices for hospital personnel and secure patient data; they can be configured as First Responder devices for Fire and Police personnel and of course for teleworker application. The can be integrated into SCADA systems, act as secure video surveillance platforms, or even as libraries for mobile training teams. As a platform, the Linux Boot solution is the "Swiss Army Knife" of devices. It can assume almost any role it is placed into.

3.1.8 Additional Cost – SCS devices can be covered under the current volume license agreement and therefore an additional Windows license must be purchased for each PSD purchased. The virtual guest could be used from the existing Volume License Agreement with Microsoft and would not represent any additional expense. The only time any additional cost would be incurred would be if there was a license cost for a particular program and that license was not already purchased by the customer.

3.1.9 **Tamper Resistance –** Both devices are physically tamper resistant. They both are hardware encrypted and physical excavation of the devices will render them useless. Since we have multiple OEM's there are subtle differences to the physical structure of the device. The customer, on presentation of the devices can choose which one is best suited to the Military environment. That environment may be a mix of different OEM styles based on operational environment. Tamper resistance of Linux boot devices is a bit more robust when it comes to insider threat. When using Linux devices, a user will not be able to "break out" of the security constraints they are placed within. With a Windows VM device, a skilled user could potentially cause the device to start searching for new hardware devices and place the security of the device in question by opening it to contamination from another device.

3.1.10 **Remote Disable/Delete –** allows administrators to remotely disable or delete lost, stolen or compromised devices to protect sensitive information and prevent data breaches.

3.1.11 **Password Management –** allows administrators to manage a variety of password functions including: password length, strength, expiration, invalid login attempts, and master password. Passwords can also be changed or updated remotely to help users recover forgotten passwords and also meet new security policies.

3.1.12 **Remote Provisioning –** Remotely manage security policy changes from a single location. Control password complexity, password expiration, online and offline access, and more.

3.1.13 **Offline Restrictions –** Control whether devices can be used offline. Prevent unauthorized use in external networks.

3.1.14 **IP and Domain Control –** Manage which IP and/or domains are allowable for devices to access via whitelist and blacklist methodology.

3.1.15 **Auditing and Reporting –** enforces a full audit trail with detailed graphical reporting and the ability to export both customizable audit logs and graphs for external analysis to ensure proper compliance.

3.1.16 **Advanced Filtering –** Quickly locate devices within the management console for efficient work flow. Advanced filters allow an administrator to quickly navigate through thousands devices within a matter of seconds.

3.1.17 **Active Directory Support –** Improve initial provisioning and deployment with Microsoft Active Directory support.

3.1.18 **Messaging/E-mail Alerts –** Remotely send messages to devices in the field with informative messages or announcements for workers to see when they have their SCS device connected. Also, setup e-mail alerts to notify administrators when certain events take place. (i.e.- device deleted, password changed, etc.)

3.1.19 **Secure Tunnel -** All communication occurs over secure SSL or TLS channel.

Section 4 — Use Case Studies

In this section, we demonstrate how the solution might operate under different operating conditions within environment and integrate with current Information Assurance (IA) Computer Network Defense (CND) and forensic tools that can be leveraged to enhance its capabilities.

Use Case Study 1: An law enforcement agent is assigned to investigate a possible computer crime. That agent normally has to gather his arsenal of tools when he travels. He needs a laptop, his media library, investigative tools, etc. With the PSD solution, there is no media to gather or lose or get scratched. It is all contained on the key, securely stored in a partition that only the agent can access. The authentication to this partition is ensured by up to three factors of authentication. The agent simply collects his laptop and his key and goes. All the tools needed are with the agent and he can begin immediately after arriving at his destination.

Use Case Study 2: While deployed overseas, a worker for a Fortune 500 company needs to access sensitive information across the Internet and a secured platform to access it from. Even though he may have his company issued laptop, that laptop is not secured and any information stored on it is vulnerable if it is lost or stolen. With the PSD solution, the user can have a completely sterile laptop and still have sensitive information with him at all times. The laptop merely becomes the presentation layer for the “real” computer located within the PSD key. The virtual machine on the key can be configured to fully mirror the capabilities of ANY computer the user would normally carry. Also, because of the strong 3 factor authentication capabilities coupled with the onboard hardware encryption, the data is SECURE even if the key is lost or stolen and can be recovered from the enterprise quickly and easily. The virtual machine can carry ALL the associated files and media that the user would normally carry AND provide stronger security measures.

Use Case Study 3: A member of a SEAL Team is deployed to hostile area where his communications are subject to monitoring; he runs the risk of sensitive or case information being compromised or at the very least someone “eavesdropping” on his communications. With the PSD, the operator, using his hardware encrypted virtual machine, launches a unique virtual private network (VPN) solution contained within the virtual environment. His communications are transmitted via an AES-256 encrypted tunnel that both hides his identity AND conceals his location. That encrypted communication ensures no one can intercept his transmissions and listen in on them.

Use Case Study 4: The Washington, DC area is shut down due to a snow storm. Personnel assigned to this area are told that facilities will be closed indefinitely until

it is safe to travel to them. Normally this means that there is countless lost man-days as personnel sit at home and wait to return to their duty station. If personnel were issued portable systems devices as a remote worker solution, they could simply insert the PSD into their home computer or laptop and be instantly and securely connected back to the corporate or Government environment without the risk of contamination from their personal computer.

Use Case Study 5: Within a regional medical facility or a University Health System, there is the need to protect. Data breaches like those seen at the Veterans Administrations could seriously impact the identity security the patients under their care. With a PSD, a patient would have their entire Personal Health Record (PHR) or Personnel record with them at all times. This would negate one of the longest standing vulnerabilities of a military member. Health records or personnel records in a hardware encrypted format on a device means no more carrying around the original paper copies of their records which puts those records at risk for loss, theft, damage or destruction. When checking into a healthcare facility, the patient sailor simply uses a PSD to update his record status and check into the facility. When the patient action is complete, the device is updated with the new/updated information.

These are but a few of the use cases for the PSD. There are countless more applications for the device. The device can quickly morph to become almost any set of tools or even a virtual computing environment.

.

Product Comparison

Feature	Capability	McAfee "NMCI on a Stick"	MobiKey**
16 / 32 / 64 GB sizes	√		
Preboot Authentication	√	√	
Choice of Operating System	√		
Customizable Virtual OS	√		
	√		
Robust Security	√	√	√
FIPS 140-2 (3) 2011	√		
DISA STIG	√		
Common Criteria 2011	√		
CAC Enabled	√	√	
Master Password	√		
User Password	√		
Role based permission	√		
Wipe device data	√		
Tamper Resistance	√		
Security Administration	√	√	
	√		
Device Role Customization	√	√	
Enterprise Manageable	√		
Support for multiple Administrators	√		
System wide policies	√		
Reset to default configuration	√	√	
Network / remote management	√	√	
Update Device version	√		
White list / Blacklist	√		
Disable device	√		
Remote Disable / Delete	√		
Password Management	√		
Remote Management	√	√	
Offline Restrictions	√		
Audit and Reporting	√		
Advance Filtering	√		
Message / Email Alerts	√		
Requires Internet		√	√

Section 5 — Conclusion

In conclusion both types of device configuration have a place within the a corporate, law enforcement, government, military, medical or even home computing environments. It is the key to teleworking on a secure environment from an untrusted computer (IE: A users home PC) or performing even the most demanding tasks such as forensic acquisition from a trusted, secure, and portable source. In events like the ones that have been seen in the Washington, DC area over the last couple of years, when personnel are not able to reach their assigned work location due to severe inclement weather, devices like this would have proven themselves invaluable.

Now, personnel can work from their homes while still working from a secure, trusted platform even though the physical device they were working on would have been untrusted. Personnel on travel can be issued devices in order to ensure they were working from a secure, trusted platform even though they were on untrusted or foreign host computers. First responders could use the device as part of their kit that would allow them to carry libraries or other sensitive data without the need for physical media that could be lost or destroyed. The scenarios are endless.

The main benefit here is that the devices are virtual. The benefits of virtual computing would immediately be beneficial to the Navy. Those benefits are:

- Huge cost savings in equipment, electrical, and personnel.
- Improved Information Assurance standards
- Enhanced access controls by implementing additional authentication methods
- Can use up to 75% less physical space
- Can use up to 75% less physical equipment
- Up to 40% reduction in manpower
- Rapid deployment capability
- Quickly load, copy, or restore a virtual machine to another host
- Maintain virtual libraries without the need for physical media
- Over 150 preconfigured virtual machines created and tested to DOD standards.
- Ability to transform a physical host computer into a virtual computer and mass produce it
- Rapid transition back to full capability from a Disaster Recovery scenario

Section 6 — Contact Information

Sky Catcher Solutions

P.O. Box 183 Rutherfordton, NC 21839

http://www.skycatcher.com

Contact Person: Kent Covington

Kent.covington@skycatcher.com