Providing Non-Attribution Services Ensuring Data Access and Integrity

Understanding new information threats to the Government and how it impacts your agency now.

An Anonymizer White Paper for CIFA

Executive Summary

Six months of intelligence down the drain from a blown operation…

An exposed cover…

Agents' lives on the line…

Millions of dollars lost…

How could something like this happen? Consider the following scenario:

A U.S. agent received an anonymous tip about a new extremist Web site and checked it out. The source was right – the site was recruiting for a new terrorist cell. He investigated the site, initiated contact and sent in a field agent. But as it turns out, it wasn't that simple.

The terrorists actually built a site just for the agent called a "honey pot". Then they phoned in the tip and watched as government agents and analysts visited their site. They collected IP addresses from the government's internal networks and used that to discover locations, plant tracking cookies, and more. With this information, the terrorists were able to social engineer more information. It all started with the exposed IP address.

If the agents had shielded their IP address when they investigated the site, the terrorists never could have spotted them, obtained their internal IP addresses, or monitored their online activities. *Internet Counter-Intelligence* involves using a series of sophisticated tools called *Web Analytics* to uncover government user identities by analyzing and tracking online activities, and capturing IP addresses and network identities.

Protecting the government enterprise from these identity threats involves completely hiding your corporate network identity from the prying eyes of competitors and others who have intentions of "ill will" against your organization. To provide true masking capability entails more than another hardware or software enhancement for your existing network infrastructure. It requires a complete solution that today's most sophisticated Web analytic tools will be unable to thwart.

These IP addresses are easy to spot as thousands of IP addresses for agencies are freely available and published on the Internet (see Appendix A).These lists are created by individuals who assist users in blocking or spoofing government analysts and agents accessing their sites. These turn-key solutions make it simple for Web administrators to determine who their site visitors are and automatically block or alter their site based on the visiting IP addresses.

The following threats illustrate the repercussions you face when your online identity is not protected.

IP-Based Blocking – A Web site can block incoming requests based on an agency's IP address or simply make it look like the Web site no longer exists. *Example* – The Department of Justice is investigating a fraud case and they visit a suspect Web site. By so doing, they expose the agency's IP address to the administrators of the unlawful Web site, thereby alerting them to the fact that they are under investigation. The Web administrators can then employ a variety of counter measures - they can either block further access by the investigators to the site or make it appear as though it no longer exists. Therefore, by simply exposing the IP address the analyst inadvertently provided the administrators with valuable information and potentially compromised the entire investigation.

IP-Based Cloaking – A Web site can change its online content based on a user's IP address or geographic location. *Example* – An agent received a tip that a Web site is selling counterfeit goods online. When the agent visits the site, it is able to detect the visitor is with the government and automatically changes the

content to hide the counterfeit merchandise. The mere fact that a government agent is visiting pages on a particular site, and disclosing their IP address, could compromise an operation.

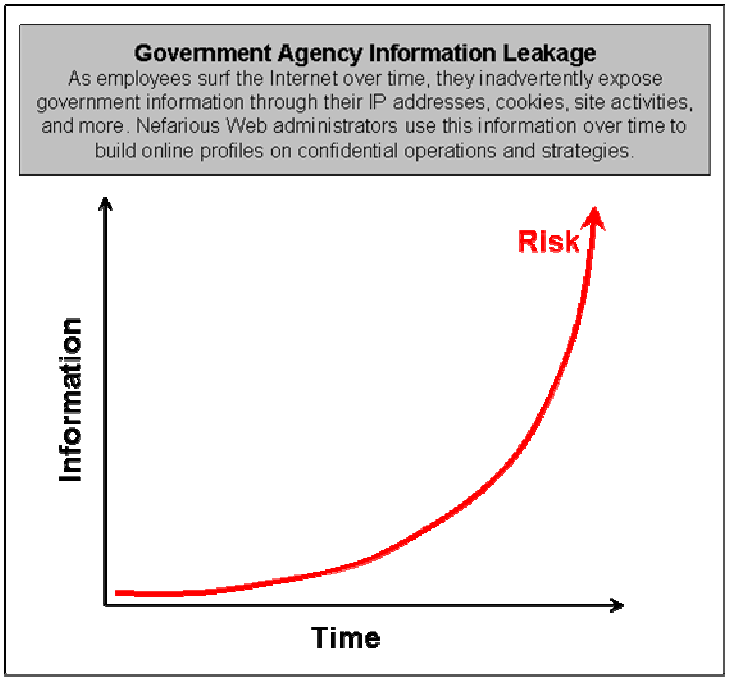
Cyber Terrorism - Cyber Terrorism refers to the direct intervention of a threat source towards your government Web site. *Example* – In 1997, the Pentagon simulated a cyber attack and found that attackers using ordinary computers and widely available software could disrupt military communications, electrical power, and 9-1-1 networks in several American cities. Hacking tools and expertise have become only more widespread and increasingly sophisticated since then.

Anonymizer® solutions circumvent these aforementioned threats by completely masking the network identity while users are online. This is accomplished by combining secure high-performance network access, the use of variable IP addresses, and the application of pre-registered domain names. These features make it statistically impossible for any organization to trace back and uncover their true government identity.

Introduction

What is Internet Counter-Intelligence? This new threat involves using the Internet and a series of sophisticated tools called *Web Analytics* to uncover government user identities by analyzing and tracking surfing habits, and by capturing IP addresses and network identities in an effort to obtain confidential information. Government agencies need to mitigate this threat or risk undermining their covert and overt operations.

Today, your staff would never consider utilizing the Internet "naked" — without a reliable anti-virus software and firewall solution installed on their PC's and networks. However, they are visiting Web sites equally unprotected in other ways, exposing their IP addresses and network identities to Web site administrators. In addition, when a user visits a Web site, they also disclose their operating system, browser version, physical address and anything that might be saved to their clipboard. This could result in an exposed cover, millions of dollars lost, or even risk the lives of your agents.



Over time, the risks associated with the above threats increase as the amount of data collected on your agency's online activities increases. Anonymizer, the leader in online identity protection and information assurance, wants government users like yourself to be aware of the threat of Internet Counter-Intelligence and help you understand the magnitude of the dangers that are inherent when utilizing the Internet without protection.

Anonymizer Government Solutions and their Advantages

Protecting government agencies from these identity threats involves protecting your network identity from the prying eyes of those who have intentions of "ill will" against your organization. To provide true protection capability entails more than another hardware or software enhancement for your existing network infrastructure. It requires a complete solution that today's most sophisticated Web analytic tools will be unable to thwart.

Anonymizer provides government agencies protection by combining key components that aid in protecting their identities and their confidential information:

- **Anonymous IP Addresses** - Anonymizer utilizes thousands of IP addresses from several sources to protect and hide the identity of all its customers while they are using the Anonymizer Network. Customers are even able to look as though they're coming from a different region of the world such as the Middle East.

- **Rotating IP Addresses** – Anonymizer uses a variety of techniques that alter how IP addresses are assigned to customers when they sign on to the Anonymizer Network. Since the user's IP address changes on a frequent basis, it is impossible for another site to detect their true identity.

- **Discreet Domain Names** – Anonymizer uses a number of pre-registered small business domain names that appear like everyday traffic and cannot be traced back and reveal your actual domain identity. This ensures complete protection from unwanted surveillance.

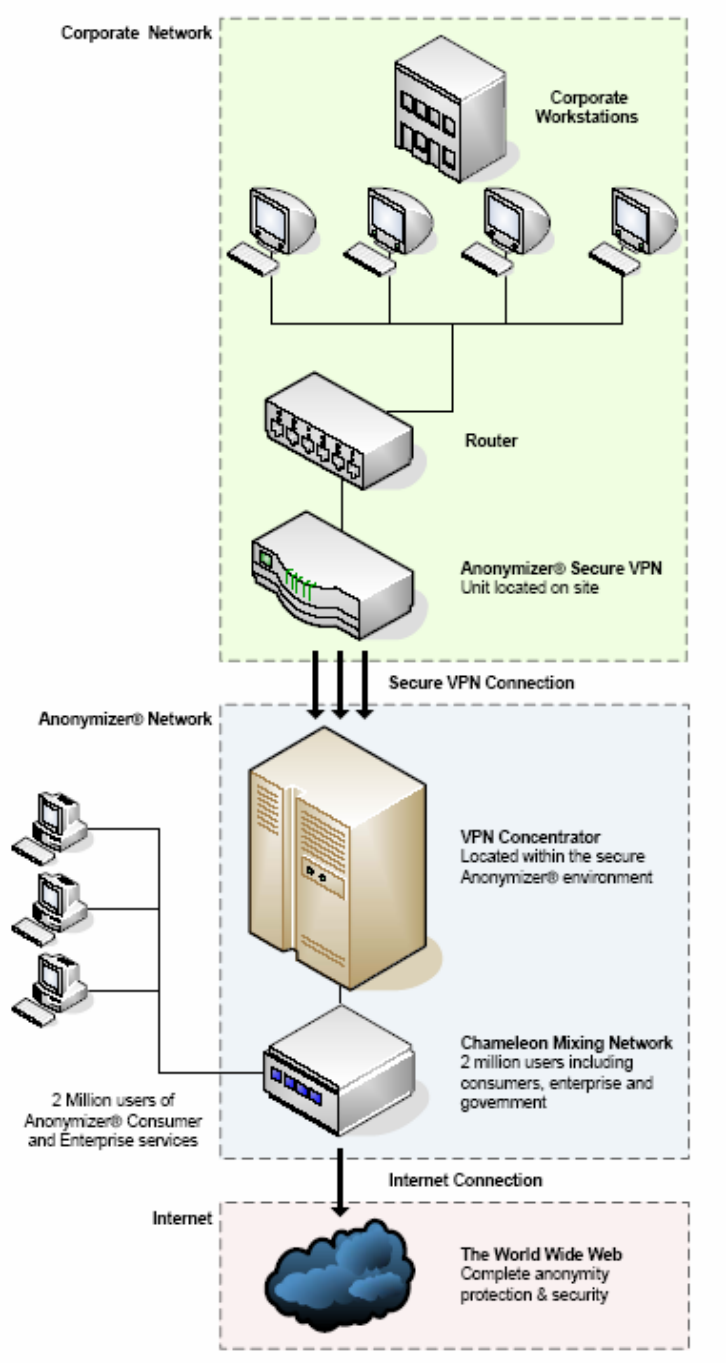
- **Fast and Secure Network Infrastructure** – Anonymizer combines ample bandwidth along with a highly secure VPN encryption to ensure that your network identity is afforded fast and secure communications, which cannot be traced back or identified in any way. In addition, Anonymizer provides full data redundancy, ensuring that your Web-based information is safe and secure.

- **Trusted Protection** - Anonymizer has been the trusted leader in identity protection and information assurance since 1995, without a single security breach to date.

The features that Anonymizer builds into its network design to ensure non-attribution make it statistically impossible for any organization to uncover the true identity of your agency.

To provide government agencies with the widest possible choice of solutions to meet their information gathering needs, Anonymizer provides four levels of identity protection and information assurance solutions geared toward the organization's anticipated usage requirements.

The first is the Anonymizer Enterprise Chameleon™ which is explained in detail below.



The Anonymizer Enterprise Chameleon

Anonymizer Enterprise Chameleon is the perfect solution for government users to protect their identities while engaging in Internet activity. This solution can be implemented to protect individual analysts, single departments or entire organizations. It works with all ports and protocols, ensuring fast and flawless Internet access.

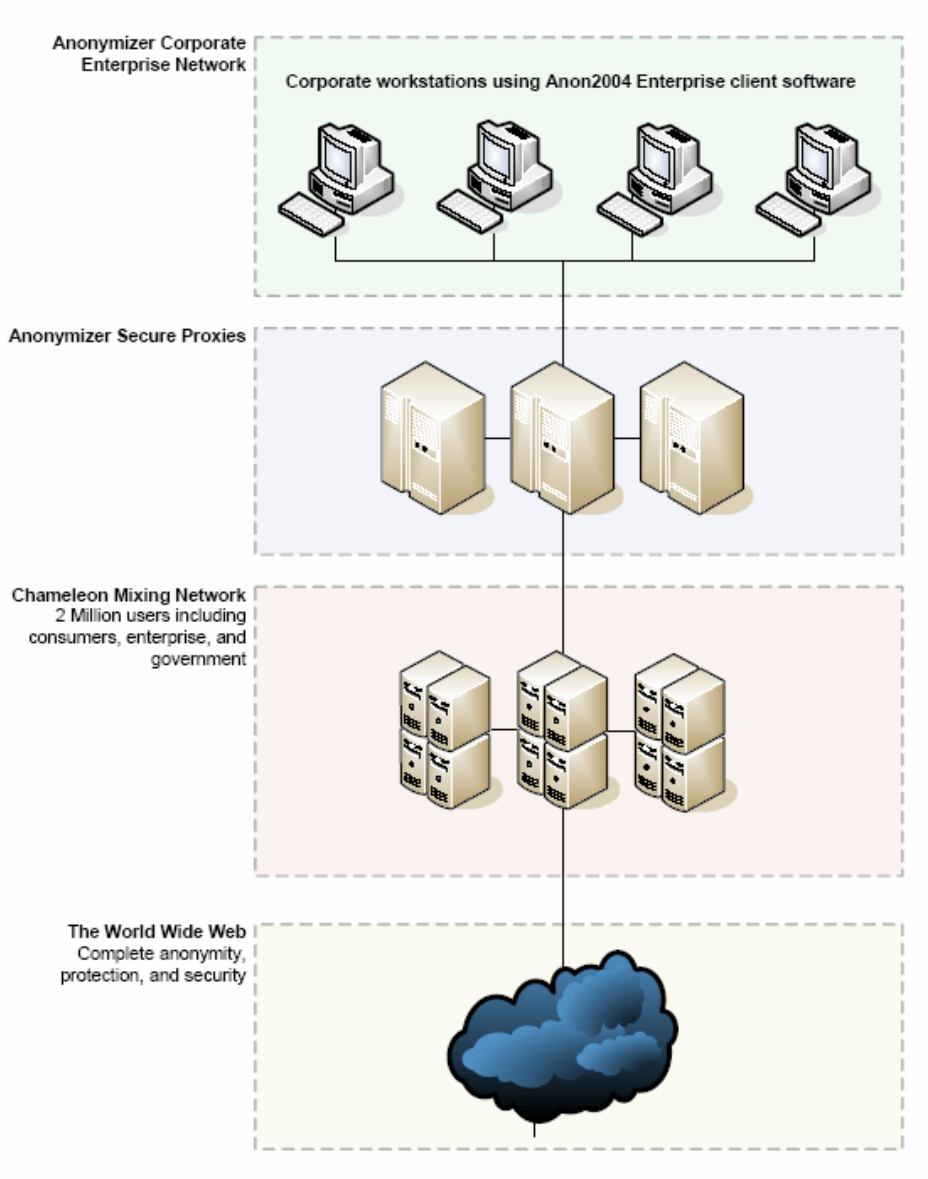
With the Enterprise Chameleon, a secure Virtual Private Network (VPN) network router is attached to the enterprise network. All network traffic is then rerouted to Anonymizer's Chameleon Network, protecting users 24/7.

The Anonymizer Enterprise Chameleon uses a technique called "IP Rotation" where the IP address that is used for the subscriber's network is changed on a daily or periodic basis. This is best suited for organizations that perform a significant amount of competitive analysis on the Web and need to covertly access competitive or industry Web sites without their knowledge.

A Network Access Translation module (NAT) dynamically controls the IP address that is presented to the outside world. The IP addresses are rotated daily and custom rotation frequencies are available for an additional fee.

IT organizations can determine how many users will be allowed to tunnel through this VPN at any given time, whether executives only, the analysts, or the entire government agency.

The second identity protection solution for the government is the Anonymizer Enterprise Client Chameleon™.



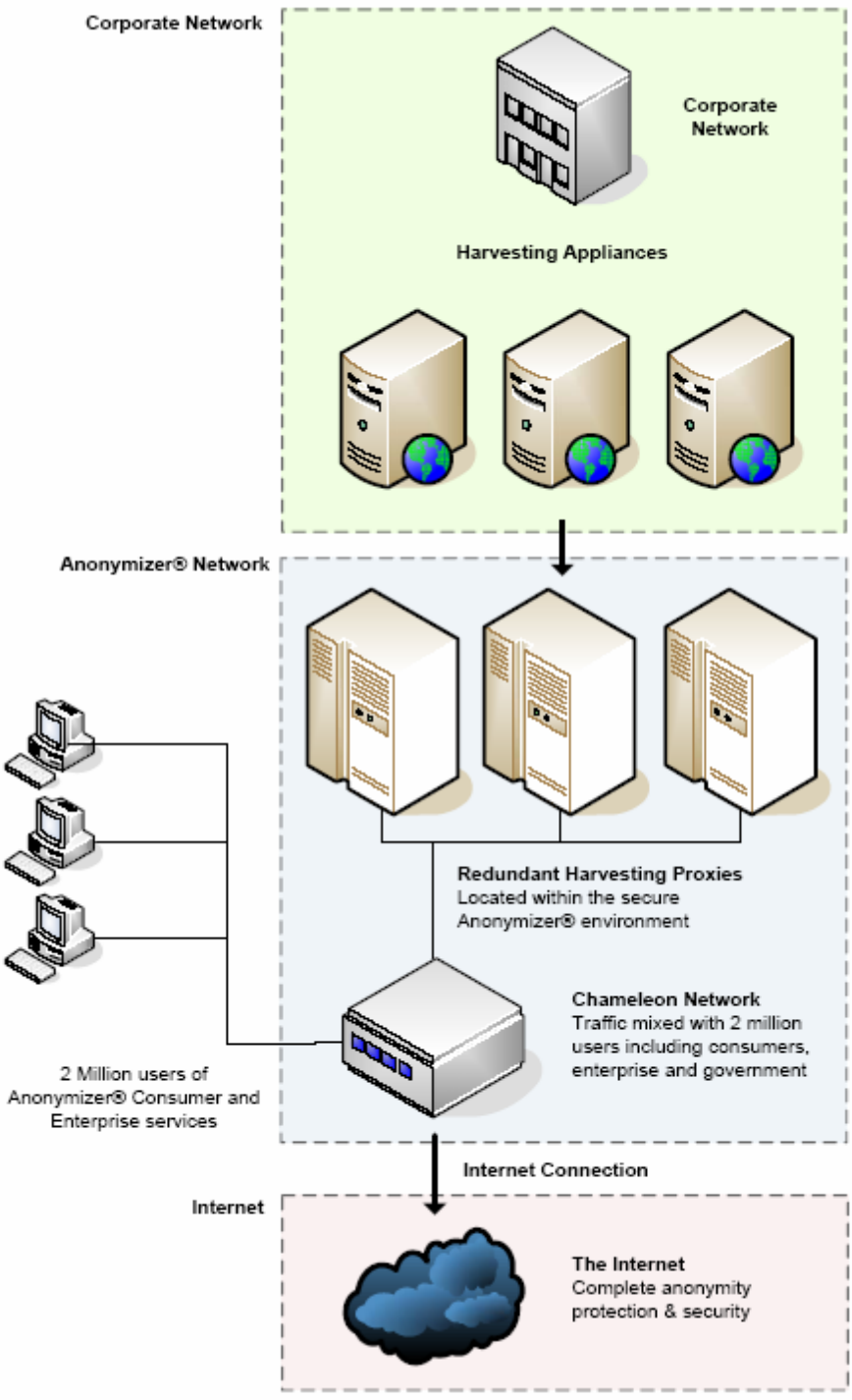
The Anonymizer Enterprise Client Chameleon

The Anonymizer Enterprise Client Chameleon is a must-have for those who work remotely and want to protect their identity while surfing the Internet, such as field agents.

The Enterprise Client Chameleon is provided as a CD that is installed on select client devices. This solution provides a “toggle-like” software switch that allows the user to turn the solution on or off at will. This is especially useful for remote or mobile users who have laptop or notebook computers. These users may access enterprise information from home or on the road, raising the risk of exposing their identities in unprotected network environments such as wireless cafes or hotels.

This solution is also useful for smaller organizations that require a simple solution for a limited number of users.

The third identity protection solution for the government is the Anonymizer Intelligence Chameleon™.



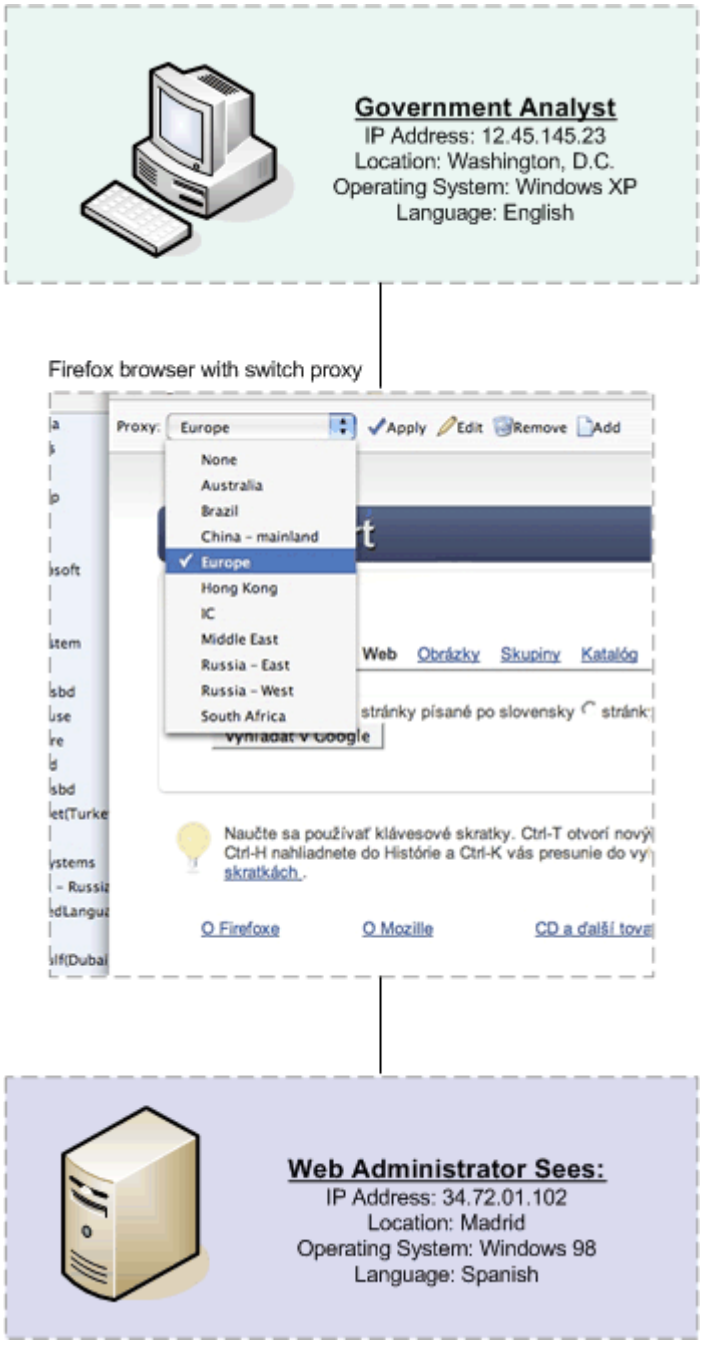
The Anonymizer Intelligence Chameleon

The Anonymizer Intelligence Chameleon is the perfect solution for any government organization that uses Unstructured Data Management (UDM) tools to conduct automated Web harvesting research.

The Intelligence Chameleon uses a technique called “IP Explosion” which causes each TCP network connection to go out on a randomly selected IP address from a pool of thousands of addresses.

The Intelligence Chameleon can be used with or without an attached VPN, providing organizations flexibility in setup.

The fourth identity protection solution for the government is Anonymizer's Geographic Distribution™.



Anonymizer Geographic Distribution

Anonymizer Geographic Distribution is a necessary tool for any government analysts or agents that are researching Web sites and wish to conceal their true geographic location.

As explained earlier, Web administrators can automatically change the content of their Web sites based on a visitor's IP address or geographic location. For example, a terrorist cell could change the content of their Web site to appear benign when someone from the United States visits their site.

This online tool provides users the ability to change the information that is provided to Web administrators through simple reverse lookup. Geographic Distribution enables users to select a country of origin in addition to the operating system, language and time zone. Thus, users could appear as if they are located in Madrid and all of the corresponding information would be provided seamlessly.

Anonymizer has Geographic Distribution locations in the following countries:

- Slovakia
- Turkey
- Additional countries added for customer requirements

Summary

Anonymizer currently works with the intelligence community throughout the United States providing our Net Chameleon services to analysts and agents in organizations that conduct research and investigations online. Through our Chameleon proxy service Anonymizer's Network Privacy Solution prevents the tracking of government usage and government identification while accessing the Internet. Our computer identity is something we take for granted each time we log onto the Internet. The ease of accessing information on the Web has created a false sense of security that can be exploited by online snoops, hackers, and cyber terrorists using new and powerful tools at their disposal. The government must protect against the threats imposed by Internet Counter-Intelligence. The only way to circumvent this threat is to completely mask user identities, making this a new requirement while online. To maintain productivity standards and achieve the desired results of the DODIIS community, it is imperative for all intelligence organizations to conduct research anonymously allowing them to harvest information in the quantities that they require. This is only possible through an infrastructure that is highly available, secure, scalable and manageable.

The Anonymizer Chameleon Network allows your staff to discretely gain uninterrupted access to public information. By leveraging discreet domain names and IP addresses, Anonymizer prevents outside parties from distinguishing your identity from any other user on the Internet. This provides a level of assurance that your employees will have completely accurate and unfettered access to all forms of Internet-based information without compromising confidentiality or jeopardizing an operation.

To summarize, there are three advantages associated with using Anonymizer for your Identity security:

- **Protects Government Identity** – Anonymizer ensures that your online research/investigative activities and Internet destinations remain anonymous and uncompromised.

- **Enables Accurate Investigative Research** – With Anonymizer, the accuracy of your research is guaranteed without concern that your organization's identity will expose your analysts to false information that is being modified.

- **Prevents Preemptive Competitive Action** – Anonymizer ensures that your agency's identity will remain completely protected, preventing any third parties from taking any pre-emptive actions that might cause compromise your operation or harm your agents.

About Anonymizer

Anonymizer, the most trusted name in privacy, defends consumers, businesses and government agencies with comprehensive online identity protection solutions ensuring their privacy while using the Internet. Anonymizer identity protection solutions have secured millions of users since 1995 without a single security breach, while providing information assurance and control over their online identities.

As Internet technology advances, online threats such as identity theft, user profiling, IP-based cloaking and cyber-terrorism grow exponentially. Anonymizer identity protection solutions mitigate these threats and ensure a safe and secure Internet experience. For more information, please visit our Web site at www.anonymizer.com/enterprise.

5694 Mission Center Road #426
San Diego, CA 92108-4380 (888) 270-0141
www.anonymizer.com/enterprise