Department of Justice

STATEMENT OF

RICHARD W. DOWNING
DEPUTY CHIEF
COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, AND NATIONAL SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED:

"CYBERSECURITY: PROTECTING AMERICA'S NEW FRONTIER"

PRESENTED

NOVEMBER 15, 2011

Statement Of
Richard W. Downing
Deputy Chief
Computer Crime and Intellectual Property Section
Criminal Division

Committee on Judiciary
Subcommittee on Crime, Terrorism, and National Security
United States House of Representatives

"Cybersecurity: Protecting America's New Frontier"
November 15, 2011

Good afternoon, Chairman Sensenbrenner, Ranking Member Scott, and Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice.

As the Committee is well aware, the United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and limited comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Our critical infrastructure – such as the electrical grid, financial sector, and transportation networks that underpin our economic and national security – have suffered repeated cyber intrusions, and cyber crime has increased dramatically over the last decade. Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain.

Recognizing the serious nature of this challenge, the President made cybersecurity an Administration priority upon taking office. During the release of his Cyberspace Policy Review in 2009, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." The President also highlighted the importance of sharing responsibility for cybersecurity, working with industry to find solutions that improve security and promote prosperity.

Over the past two years, the Administration has taken significant steps to ensure that Americans, our businesses, and our government are building better protections against cyber threats. Through this ongoing work, it has become clear that our Nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated, including the Computer Fraud and Abuse Act ("CFAA").

Members from both sides of the aisle have likewise remained steadfast in their resolve to act on cybersecurity legislation. I want to particularly acknowledge your leadership, Chairman Sensenbrenner, in the effort to address these important threats. The Administration welcomes

the opportunity to assist these congressional efforts, and we have developed a pragmatic and focused cybersecurity legislative proposal for Congress to consider as it moves forward on cybersecurity legislation. This legislative proposal is the latest development in the steady stream of progress we are making in securing cyberspace.

The proposed legislation is focused on improving cybersecurity for the American people, our nation's critical infrastructure, and the federal government's own networks and computers. The aspect of the proposed legislation I want to discuss today is the revisions to the CFAA and related legislation.

The Administration's goals

Over the decades since the CFAA was originally passed, the Justice Department has worked with Congress to keep the statute up-to-date and effective. Over time, we have had several objectives in seeking reform of the CFAA, three of which are of paramount importance today.

Our first objective is to make the CFAA as technology-neutral as possible. Experience has demonstrated that advances in technology at times render statutes in the area of cyber crime obsolete. By drafting them in a technology-neutral way, they remain viable despite technological change. By contrast, statutes defined in terms of specific technologies not only require Congress to expend effort trying to keep them up-to-date, but potentially allow criminals to avoid punishment on a technicality. Our experience has shown that computer crime statutes can be written in a forward-thinking way that accounts for technological change, yet sets forth "rules of the road" that make clear the line between criminal and non-criminal conduct.

Second, Congress should ensure that federal law treats conduct in the online world commensurate with similar physical-world conduct. Penalties for fraud committed using a telephone should not differ, for example, from penalties for fraud committed by computer hacking.

Third, the criminal law should provide appropriately severe penalties to promote deterrence. Computer crime is a burgeoning area of criminality that is difficult to investigate and prosecute. Criminals from across the country and around the world are taking advantage of the relative anonymity provided by the Internet to compromise our critical infrastructure, obtain trade secrets, intrude into bank accounts, and steal the personal and financial information of ordinary Americans. Where ten years ago hackers were more commonly motivated by curiosity or seeking notoriety, most criminal hackers today are motivated by greed. Federal law needs to more effectively deter this spreading criminality.

Computer crimes as a RICO predicate

We propose updating the Racketeering Influenced and Corrupt Organizations Act ("RICO") to make CFAA offenses subject to RICO. As computer technology has evolved, it has become a key tool of organized crime. Indeed, criminal organizations are operating today around the world to: hack into public and private computer systems, including systems key to national security and defense; hijack computers for the purpose of stealing identity and financial information; extort lawful businesses with threats to disrupt computers; and commit a range of other cyber crimes. Many of these criminal organizations are similarly tied to traditional Asian and Eastern European organized crime organizations.

The fight against organized crime is far from over; rather, much of the focus has moved online. RICO has been used for over forty years to prosecute organized criminals ranging from mob bosses to Hells Angels to insider traders, and its legality has been consistently upheld by the courts. Just as it has proven to be an effective tool to prosecute the leaders of these organizations who may not have been directly involved in committing the underlying crimes and to dismantle whole organizations, so too can it be an effective tool to fight criminal organizations who use online means to commit their crimes. The Administration's proposal would simply make clear that malicious activities directed at the confidentiality, integrity, and availability of computers should be considered criminal activities under the RICO statute.

Simplifying the CFAA to appropriately address culpable individuals

The Administration proposal would make a number of changes to the CFAA's sentencing provisions. The goal of these changes is to eliminate overly complex, confusing provisions, simplify the sentencing scheme, and enhance penalties in certain areas where the statutory maximums no longer reflect the severity of these crimes.

First, the proposal would clarify that conspiracy to commit a computer hacking offense is subject to the same potential maximum penalty as a completed, substantive offense. Whether or not a cyber criminal is the person who actually "pushed the buttons" to commit the crime should not matter – the intent of the criminal to commit a serious computer crime is what counts. Indeed, in many of the investigations and prosecutions being handled by the Department today, the most culpable figures are not the lower-level operatives who physically execute a criminal scheme but the leaders who make the key decisions and earn the lion's share of the illicit proceeds. This proposed change would provide greater deterrence by enhancing certain penalties.

Second, we also believe that the penalty provisions in the CFAA should be simplified by removing references to subsequent convictions in favor of setting an appropriate maximum sentence for each offense. In general, the maximum would be the number of years currently designated for a second offense. This approach would eliminate needless complexity in the sentencing scheme and free federal judges to provide appropriate sentences to first-time offenders in instances where the crime was extremely serious or resulted in widespread damage.

Third, our proposal would increase the maximum penalties in several cases to give judges the authority they need to adequately punish serious offenders and to make these penalties commensurate with the same type of conduct occurring off-line. We believe that such modifications are appropriate in light of the scale and scope of our nation's current cyber crime problem.

Moreover, some of the CFAA's sentencing provisions no longer parallel the sentencing provisions for their equivalent traditional crimes. For example, the current maximum punishment for a violation of section 1030(a)(4) (computer hacking in furtherance of a crime of fraud) is five years, but the most analogous "traditional" statutes, 18 U.S.C. §§ 1341 and 1343 (mail and wire fraud), both impose maximum penalties of twenty years.

Indeed, for a serious computer crime offense, it is easy to imagine scenarios in which the appropriate sentence exceeds the current maximum. For example, were a criminal to steal a massive database of credit cards, the maximum penalty under section 1030(a)(2) for that crime is five years in prison, even though the United States Sentencing Guidelines might recommend a much higher sentence. In other words, in such situations, a federal judge would be prevented from sentencing a defendant to an appropriate prison term that will assure proper punishment and promote general deterrence.

All of these changes will empower federal judges to appropriately punish offenders who commit extremely serious crimes, ones that result in widespread damage, or both. Judges would still make sentencing decisions on a case-by-case basis, and defendants would still have the right to appeal any sentence deemed excessive or unreasonable.

Updated tools for investigators and prosecutors

Further, we believe that the CFAA currently has limitations that have prevented it from being used fully by prosecutors against criminals that steal login credentials, such as user names, passwords, or secure login devices. These shortcomings should be corrected. The Administration proposes that the scope of the offense for trafficking in passwords in the CFAA (18 U.S.C. §1030(a)(6)) should cover not only passwords but other methods of confirming a user's identity, such as biometric data, single-use passcodes, or smart cards used to access an account. It should also cover login credentials used to access to any "protected" computer (defined in the statute quite broadly), not just government systems or computers at financial institutions.

This proposal will help equip law enforcement to fight a key area of cyber crime: the theft of passwords and means of access for the purpose of committing additional crimes, such as wire fraud and identity theft. Expanding this definition will improve the ability of federal prosecutors to prosecute these offenders. It will also keep the CFAA up-to-date with changing technology. For instance, if in ten years iris scans have taken the place of passwords as the main method for managing credentials to computer systems, Congress will not have to act because the Administration's proposal would have made the CFAA technology-neutral, allowing it to adapt

to technological change.

Finally, we propose several amendments to the CFAA related to forfeiture. Key amongst these changes would be the addition of a civil forfeiture provision to the CFAA. Unlike most federal criminal statutes with forfeiture provisions, currently the CFAA only provides for criminal, and not civil, forfeiture. This forces federal prosecutors to use criminal forfeiture authority in instances where civil forfeiture would be more appropriate or efficient. The Administration also requests other modest changes to the CFAA forfeiture subsection, namely to clarify that the "proceeds" forfeitable under the CFAA are gross proceeds, as opposed to net proceeds, and allow forfeiture of real property used to facilitate CFAA offenses in appropriate cases.

The proposed civil forfeiture provision is consistent with similar provisions in federal law that have existed for decades. It should also be noted that any use of civil forfeiture authority by the government is subject to both the "innocent owner" defense – which applies when an owner claims that they are innocent of a crime and therefore their property should not be forfeited – and proportionality review under the Eighth Amendment.

Amending the statute to cover "gross" proceeds is also a reasonable clarification. Criminal enterprises should not enjoy the benefits of the ordinary accounting standards and tax rules used by legitimate businesses. All of the monies earned from the crime should qualify for forfeiture because criminals should not be allowed to "deduct" the expenses of operating their criminal enterprise. For example, a drug dealer who buys an expensive car should not be entitled to deduct the price of the car as a cost of doing business.

Enhanced deterrence for malicious activity directed at critical infrastructure

Finally, we recommend strengthening the criminal code to better deter malicious activities directed at computers and networks that control our critical infrastructures. Critical infrastructure consists of the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, national economic security, or public health and safety.

America's open and technologically complex society includes, as a part of its critical infrastructure, numerous vulnerable targets. A significant portion of these are owned and operated by the private sector and state or local governments. These critical infrastructure systems are vulnerable to destruction, incapacitation, or exploitation by a variety of malicious actors, which poses grave risks to our national and economic security. Ordinary criminals could also take advantage of potential vulnerabilities in our critical infrastructure for purposes of extortion.

Specifically, computerized control systems perform vital functions for the critical infrastructure. They are vital in areas ranging from monitoring the distribution and quality of

drinking water to ensuring the safe operation of nuclear power plants. For example, in natural gas distribution, such systems can monitor and control the pressure and flow of gas through pipelines. If a criminal or terrorist seized control of those systems, he or she could potentially disrupt the energy supply or cause an explosion. As the Committee knows, the CFAA creates maximum penalties for malicious activity directed at the confidentiality, integrity, and availability of computers. While these crimes currently apply to the computers and networks that run our critical infrastructure, they do not require any mandatory minimum penalty for such conduct. While it is reasonable to believe that courts would impose appropriate prison terms if malicious activity severely debilitates a critical infrastructure system, it is possible that courts might not impose adequate penalties for activities that cause less disruption – or none at all in the case of an attempt that is thwarted before it is completed.

In light of the grave risk posed by those who might compromise our critical infrastructure, even an unsuccessful attempt at damaging our nation's critical infrastructure merits substantial penalties. The Administration has proposed a mandatory minimum sentence of three years imprisonment as one appropriate way to achieve the needed deterrence. We understand that members of the Committee have raised concerns about mandatory minimum sentencing in general. We are, as always, happy to work with this Committee to explore potential alternatives to a mandatory minimum for attacks on critical infrastructure that not only appropriately punish offenders, but also more effectively deter others who would engage in such misconduct that puts public safety and national security at risk. In whatever form it would ultimately take, the message needs to be sent loud and clear to criminals and other malicious actors that any attempt to damage a vital national resource will result in serious consequences.

Restricting substantive definitions in the CFAA will make it harder to address insider threats

Finally, on behalf of the Department I want to address concerns regarding the scope of the CFAA in the context of the definition of "exceeds authorized access." In short, the statute permits the government to charge a person with violating the CFAA when that person has exceeded his access by violating the access rules put in place by the computer owner and then commits fraud or obtains information. Some have argued that this can lead to prosecutions based upon "mere" violations of website terms of service or use policies. As a result, some have argued that the definition of "exceeds authorized access" in the CFAA should be restricted to disallow prosecutions based upon a violation of contractual agreements with an employer or service provider. We appreciate this view, but we are concerned that that restricting the statute in this way would make it difficult or impossible to deter and address serious insider threats through prosecution.

All types of employees in both the private and public sector – from credit card customer service representatives, to government employees processing tax returns, passports, and criminal records, to intelligence analysts handling sensitive material – require access to databases containing large amounts of highly personal and otherwise sensitive data. In most cases,

employers communicate clear and reasonable restrictions on the purposes for which that data may be accessed. The Department has prosecuted numerous cases involving insiders in both the public and private sectors who have violated defined rules to access and obtain sensitive information. In many prosecutions involving insiders, the "terms of service" and similar rules in employment contexts define whether the individual charged was entitled to obtain or alter the information at issue. This is almost identical to prosecutions under other statutes, in which internal procedures, agreements, and communications must be examined by a fact-finder to determine, for example, whether a particular payment was authorized, or embezzlement or fraud.

Employers should be able to set and communicate access restrictions to employees and contractors with the confidence that the law will protect them when their employees or contractors exceed these restrictions to access data for a wrongful purpose. Limiting the use of such terms to define the scope of authorization would, in some instances, prevent prosecution of exactly the kind of serious insider cases the Department handles on a regular basis: situations where a government employee is given access to sensitive information stored by the State Department, Internal Revenue Service, or crime database systems subject to express access restrictions, and then violates those access restrictions to access the database for a prohibited purpose. Similarly, businesses should have confidence that they can allow customers to access certain information on the business's servers, such as information about their own orders and customer information, but that customers who intentionally exceed those limitations and obtain access to the business's proprietary information and the information of other customers can be prosecuted.

Here are three examples of recent prosecutions under the CFAA that might have been impaired if language restricting the use of terms of service had been enacted into law:

- A police officer obtained criminal history information from the National Crime Information Center database ("NCIC"), a sensitive and tightly-controlled law enforcement database which has stringent rules and regulations restricting access for official purposes. The officer then leaked the information to a defense investigator in a drug trafficking case. This unlawful conduct resulted in the conviction of the officer under the CFAA, with the Court of Appeals noting specifically that the evidence was sufficient to demonstrate that the defendant had "exceeded his authority by accessing [NCIC] for an improper purpose." (*United States v. Salum*, 257 Fed. Appx. 225, 230 (11th Cir. 2007)).

- In 2006, a contract systems administrator for Blue Cross Blue Shield of Florida used his access to the company's computer system to snoop. He initially was curious about how much his colleagues were being paid, but he proceeded to access all kinds of information, including downloading a file with hundreds of thousands of current and former employee names and Social Security Numbers. Pursuant to agreements with his employer, the administrator was obligated to keep company information confidential and to access the

information only for purposes related to his job duties. Although there was no evidence that the employee had yet disseminated the names and Social Security numbers, Blue Cross Blue Shield incurred a cost of over half a million dollars to buy credit monitoring protection for all of the company's employees. Although the employee intensely litigated the issue of whether he had "exceeded authorized access," the court rejected his arguments, and he pled guilty to one count under section 1030(a)(2).

- Up to and through 2008, seven employees of Vangent Corporation accessed the student loan records of a number of celebrities and well-known political and sports figures, include then-candidate Barack Obama, and then disclosed this information to others, including media outlets. These employees required access to the records as part of their employment, but their employment policy prohibited them from accessing the system for non-work-related purposes. Six pled guilty to exceeding authorized access under section 1030(a)(2), and a seventh was convicted following a jury trial in 2010.

These are just a few cases, but this tool is used routinely. The plain meaning of the term "exceeds authorized access," as used in the CFAA, prohibits insiders from using their otherwise legitimate access to a computer system to engage in improper and often malicious activities. We believe that Congress intended to criminalize such conduct, and we believe that deterring it continues to be important. Because of this, we are highly concerned about the effects of restricting the definition of "exceeds authorized access" in the CFAA to disallow prosecutions based upon a violation of terms of service or similar contractual agreement with an employer or provider.

Conclusion

I very much appreciate the opportunity to discuss with you our proposals to address the threat cyber crime poses to our national security, public safety, and economic prosperity. The Administration has responded to Congress' call for input on the cybersecurity legislation that our Nation needs, and we look forward to engaging with Congress and, specifically, this Committee as you move forward on this important issue.