Sarbanes Oxley Compliance Professionals Association (SOXCPA)
1200 G Street NW Suite 800 Washington, DC 20005-6705 USA
Tel: 202-449-9750 Web: www.sarbanes-oxley-association.com

Sarbanes Oxley News, December 2014

Dear Member,

Today we will start with the Statement on Proposed 2015 Budget and Strategic Plan

James R. Doty, Chairman of the PCAOB explained at the PCAOB Open Board Meeting"

The 2015 budget and related strategic plan are the result of considerable effort and thought by board members and senior programmatic staff.

I want to express my appreciation for the efforts of our Chief Administrative Officer, Suzanne Kinzer and our Chief Financial Officer, Amy Hargrett, who are both new in their roles this year.

I would also like to thank Budget Officer Jim Hearn, Yoss Missaghian and Bobbie Rose from our budget office.

Since November 2013, when the Board last updated its five-year strategic plan, we have made substantial progress on the objectives and initiatives described in our strategic plan.

This new plan and the 2015 budget together will allow us to redouble our efforts on a number of key strategies to achieve our mission.

In particular, the new plan and budget will allow us to deepen the PCAOB's use of data, information technology and economic analysis in standard - setting and other activities.

That capacity will promote more fluid interaction among the PCAOB's programs in order to better leverage data and insights obtained through its programs.

We will also continue to expand the interim Broker-Dealer Audit Inspection Program while working to establish the permanent program.

Let me say a word about economics.

In November 2013, we formed a Center for Economic Analysis.

We have begun to staff the Center with both permanent staff and research fellows, and we are now poised to deepen our use of economic analysis in all our programs, particularly in the area of standard-setting, as well as to spur economic research on the role of auditing in capital markets and capital formation.

Economic considerations underlie the audit, but we need to know more about the levers that move auditor incentives.

Last week, a meeting of our Standing Advisory Group heard from panels of academics, auditors and forensic experts on the general topic of the relationship of the audit and the auditor to fraud — detection and prevention.

The auditor incentives (and disincentives) were discussed in detail.

The slides of those presentations went up on our website today.

That SAG meeting was a direct response to what we heard as a growing public interest in deeper study by regulation of the conditions that spawn fraud, the pressures auditors face, and the possible levers to counter those pressures.

Regulators need to be mindful of the economic impact of their own actions.

For example, I am mindful that new audit procedures and quality control measures increase cost, which may be passed on to other market participants.

Regulators need to know these and other economic effects, in order to determine whether and what actions may most effectively and efficiently meet stated objectives.

Economics provides us a framework for that critical thinking.

It prompts us to consider alternatives, to maximize the efficiency of our actions.

A near-term focus in 2015 will be further integration of economic analysis into the PCAOB's programs and further improvements in our standard-setting program.

We are now in a position to reflect upon our more than ten years of experience in setting auditing standards and refine our processes to achieve the most effective outcomes.

For example, our new tools in economics will help us build a program to conduct post-implementation review of standards.

We will also look for ways we can build more data collection and analysis into our processes.

To this end, we have already begun to use new outreach techniques to gather information earlier in our standard-setting process, through the staff consultation papers.

We started this past summer with an OCA staff consultation paper to seek public input on the need and alternatives to address problems in auditing fair value estimates.

That paper led in short order to a thought-provoking meeting of our Standing Advisory Group, in early October, to explore questions raised in the paper with outstanding panels of experts from a variety of fields.

We can expect additional consultation papers soon on two more critical auditing topics — the going concern assumption and use of specialists.

We also need to make good use of our own, internal information, including information gleaned from the nearly 300 inspections and numerous investigations we will conduct next year, both in the U.S. and abroad, as well as our risk assessment and other oversight programs.

With the help of empirical skills from staff in the Center, I'm hopeful that we will be able to develop a better sense of the baseline in practice, which will in turn help us determine where we need to focus on compliance and where we should lift the standard for everyone.

2015 will bring more outreach to audit committees, and more attention to the means of helping them be effective in overseeing the audit. 2015 will also see a concept release on audit quality indicators.

We have great expectations of 2015.

Finally, I remain hopeful that early in 2015 we will achieve greater transparency in execution of the audit, through publication of engagement partner identity and other participating firms.

I am immensely proud of the PCAOB staff for their creativity in developing new techniques to bring to bear in their work, as well as their commitment to identifying the most effective ways to protect investors.

The 2015 Budget is lower than our 2014 Budget, reflecting the challenges we have faced in hiring.

The 2015 Budget provides for a conservative increase in staff, primarily in inspections, in light of the hiring challenge.

But the budget also provides our new administrative leadership with the resources they need to refresh and upgrade our human resources, finance, and facilities functions, to bring us to a more sustainable model.

Given all the work and support that has gone into the budget, I am comfortable that it is appropriate and should be submitted to the SEC for its approval

PCAOB Approves 2015 Budget and 2014-2018 Strategic Plan Washington, DC

The Public Company Accounting Oversight Board today approved its 2015 fiscal-year budget of approximately $250.9 million and its 2014-2018 strategic plan.

The budget is $7.5 million, or 3 percent, less than the Board's 2014 budget of $258.4 million.

"The 2015 budget reflects the Board's views about how to make optimal use of the PCAOB's strengths and opportunities, as well as our insights about strategies to improve our ability to protect investors and address challenges," said PCAOB Chairman James R. Doty.

The strategic plan serves as the foundation for the 2015 budget, and guides the PCAOB's programs and operations.

The total accounting support fee for 2015 is $226.6 million, with approximately $199.1 million allocated to public companies and $27.5 million to broker-dealers.

The budget assumes that the PCAOB will reach a 2015 year-end projected total of 851 staff.

The Division of Registration and Inspections accounts for 522 of these positions, and the Division of Enforcement and Investigations accounts for 64 positions.

As of November 21, 2014, there were 2,216 public accounting firms registered with the PCAOB, including 902 based outside the United States.

The Securities and Exchange Commission rule on the PCAOB budget requires the PCAOB to maintain a strategic plan, and the PCAOB budget is subject to SEC approval.

A summary of the 2015 budget and strategic plan will be available on the PCAOB website once the budget is submitted to the SEC for consideration.

Investors' Expectations of Regulators

Steven B. Harris, Board Member
International Auditor Regulatory Institute
Washington, DC

Thank you, Bruce. I join you and my fellow Board Members in welcoming our regulatory guests from approximately 30 jurisdictions around the world to our 8th Annual International Auditor Regulatory Institute.

At the outset, I must say that the views I express today are my own and do not necessarily reflect those of the Board or staff of the PCAOB.

I chair two investor groups — the PCAOB's Investor Advisory Group as well as the Investor and Other Stakeholders Working Group of the International Forum of Independent Audit Regulators (IFIAR).

I want to share with you some of what I am hearing from these groups.

Investors are not satisfied with the current state of audit quality.

They see the rate of audit deficiencies reported by regulators from around the world and while they are appreciative of our efforts thus far, they expect more.

In April 2014, IFIAR issued its 2013 Inspections Findings Survey.

The survey, which reflects responses from 38 independent regulators, noted that the highest number of inspection findings were in the areas of fair value measurement, internal control testing, and adequacy of financial statements and disclosures.

These results are consistent with the findings of our own PCAOB inspectors.

Investors want regulators to make sure that auditors are knowledgeable about the complexities of the business they are auditing; and to have the independence, objectivity and professional skepticism to do the job right.

They also believe auditors should be doing more to detect and expose fraud and be more actively involved in challenging management when things don't seem to be right. They want auditors "if they see something, say

something," to management, the audit committee and/or directly to investors in the audit report.

Investors want audit firms to compete on the basis of quality and not price.

As such, they support the PCAOB's initiative to identify audit quality indicators to distinguish firms from each other and thereby provide for greater competition among firms based on quality.

They also want more independent, accurate and informative audit reports.

They believe that the current pass-fail boilerplate report is no longer enough.

They want an expanded audit report that informs them about the auditor's assessment of management's estimates and judgments; discusses unusual transactions, restatements, and other changes; and includes the auditor's assessment of the quality of the company's accounting policies and practices.

In addition to the expanded auditor's report, investors want more transparency and accountability with respect to those involved in an audit engagement.

While the PCAOB is currently examining how to address these concerns, other countries currently require the identification of the audit partner in the audit report.

Investors are also concerned about the future direction of audit quality as the largest accounting firms expand into ever increasing lines of business activity that include a variety of consulting and advisory services.

As many of you are aware, the Big Four accounting firms have been continually expanding their consulting businesses, either internally or through acquisitions and some are expanding into services not generally associated with accounting firms.

For example, a foreign affiliate of a Big Four announced in March its ambitions to become a global top-20 legal services player within the next five years.

Firms have asserted that these acquisitions and investments will improve their auditing capabilities and, while this may be true, investors want to

know how these additional services will assist firms in improving audit quality.

In the United States, our Supreme Court in United States v. Arthur Young, described the audit as a "public watchdog" function that "demands that the accountant maintain total independence from the client at all times and requires complete fidelity to the public trust."

As firms broaden their activities, investor representatives I hear from are concerned that regulators and the firms alike not lose sight of this "total independence" and "public trust" responsibility.

Investors also want regulators to exercise more oversight of the global network firms and their affiliates with an enhanced focus on audit quality.

Some have suggested that the global firms change their governance structures to include more independent representation on the global firms' managing boards, something that is currently in place in a number of countries.

Investor representatives I hear from also are concerned that we may have reached a point where the largest firms may be too big to fail.

They wonder if these firms are so systemically important to the economy, that the market wouldnot allow one to fail.

Currently, certain jurisdictions around the world require that the major accounting firms provide audited financial statements.

For example, certain large accounting firms in the United Kingdom, the Netherlands and Austria include audited financial statements in their annual transparency reports, which are posted on their respective websites.

I believe, along with a number of investor representatives, that having audited financial statements may provide the necessary transparency to allow the marketplace to monitor the growth and activities of these firms and identify any catastrophic risk that may expose a firm to failure.

Investors want audit committees and their auditors to share more information among themselves, independent of management, in order to better protect their interests in receiving independent, accurate and informative audit reports.

And they would like us to carefully monitor and consider the role of the auditor regarding global initiatives to promote sustainability and integrated reporting.

In sum, these are a few of the issues that investors and others have brought to our attention.

On Wednesday, you will hear directly from a panel of investor representatives about some of their concerns.

In the end, what investors want are independent, objective, skeptical auditors watching out for their best interests through a high quality audit.

They see themselves — and believe that investors should be recognized by auditors and regulators alike — as the auditor's primary client and that protecting their interests must be the major objective of everything we do as regulators.

Thank you and I am happy to answer any questions.

The Importance and Positive Impact of Independent Audit Oversight Date:

Jeanette M. Franzel, Board Member
International Auditor Regulatory Institute
Washington, DC

Good morning, and welcome to the 8th annual PCAOB International Auditor Regulatory Institute.

You have traveled from many places around the globe to Washington, DC, to share your knowledge and points of view about audit regulation.

We have with us participants from 30 non-U.S. jurisdictions and five international organizations, in addition to those from the PCAOB, the SEC, and the U.S. Treasury Department.

We look forward to hearing from you today.

The Institute — once a place to tell you about the US experience in independent audit oversight — is, today, as much about us listening and learning from the perspectives you bring from other countries and jurisdictions.

The growth and evolution in audit regulation around the world is manifest in our changed agenda for this Institute.

The agenda reflects an interactive exchange of information, experiences, and expertise on maturing approaches to audit regulation and cooperation among independent regulators.

So, now, it may be time to ask, What has been the impact of independent audit regulation on the audit profession?

And the capital markets?

I believe the impact has been positive.

Are investors better protected as a result? I believe the answer to that is yes.

But there is a lot that still needs to be done.

During this Institute, we will discuss many areas where additional work and focus are needed.

Before I get started, as is our policy, I have to tell you that the views I express are my own and do not necessarily reflect those of the Board or staff of the PCAOB.

Need for International Regulatory Collaboration

First, let's remember how we got here: This Institute began in 2007 as a venue for representatives from independent audit regulators and government agencies to come together "to learn more about the PCAOB's programs and how it carries out its mandate under the Sarbanes-Oxley Act of 2002."

The PCAOB's continuing objective for the Institute has been "to provide a forum for open discussion about how audit regulators around the world can better protect the interests of investors and increase efficiency, reliability and transparency in accurate and reliable financial reporting."

The first Institute was held only a matter of months after 18 independent audit regulators joined together in September 2006 to establish the International Forum of Independent Audit Regulators, or IFIAR.

Since then, IFIAR has grown to 50 members, and their approaches to audit regulation have evolved as well.

I know that many of you here today represent jurisdictions that also belong to IFIAR and participate in its meetings and working groups.

Since its establishment, IFIAR's activities and the direct participation of its members have increased considerably.

And IFIAR's inspection workshop has become the primary vehicle for inspectors to share methods and experiences.

To these ends, I commend the IFIAR Chair, Lewis Ferguson, and Vice Chair, Janine van Diggelen, for their leadership in setting a clear path for IFIAR to mature as an organization that provides for robust international regulatory cooperation and information sharing.

You will hear from them about IFIAR's mission and current activities during the Institute this week.

Evolving Agenda for the Institute

This year, the Institute agenda continues to call for the PCAOB to share information about its activities and operations.

It also, however, has a heavy emphasis on dialogue among peer regulators on a variety of regulatory topics that are of shared interest.

We are honored and grateful for the participation of speakers from 11 countries and jurisdictions around the world — and a variety of other government agencies and organizations.

We look forward to discussing, among other matters, common inspection findings, European audit reforms, the role of audit in combating fraud and global corruption, the evolving audit report, and audit issues in emerging markets.

I call your attention to the evaluation form for this Institute, and I invite you to share your feedback about how we can further develop the agenda for this venue to achieve our objective of having "open discussion" in the context of evolving international regulation.

Impact of Independent Audit Regulation

Last year, in light of PCAOB's 10th anniversary, we discussed the growth and evolution of independent audit regulation around the world.

This year, I want to talk about the impact of independent audit regulation on the audit profession and the capital markets.

In other words, have the growth and evolution in independent audit regulation, since it began in earnest in 2003, had a positive impact on audit quality and the protection of investors?

The answer is an unequivocal, "yes."

Through inspections and other oversight activities, audit regulators have identified and called attention to weaknesses, risks, and challenges in the audit profession.

For example, the annual and periodic public reports of IFIAR and its members have consistently drawn sharp attention to common inspection findings around the world for the past two years.

In the United States, for example, in addition to individual inspection reports, the PCAOB has issued a number of general reports, staff audit practice alerts and other public documents that highlight a range of findings that arise during inspections of registered audit firms.

In response to such matters -- and in response to the demands of investors and other market participants for improvement in audit practice -- regulators around the world have also revised auditing standards and taken enforcement actions for violation of those standards and related laws and regulations.

There is no question that public transparency about audit deficiencies and risks has had a salutary effect on the audit profession.

The vast majority of audit firms have reacted responsibly by taking actions to improve compliance and overall audit quality.

I also believe that regulatory oversight by the PCAOB and others has driven needed improvements in auditor behavior and practices.

In my view, our actions as audit regulators have had a positive impact on audit quality.

This is not to say that we can declare success and consider the job done.

We all know there is much more to do to achieve and maintain high audit quality on a consistent basis. But we have seen positive change, and we know it is possible.

As we discussed last year, and will again this year, however, measuring any changes in audit quality is difficult. Some of our fellow regulators measure and report on progress in certain aspects of audit quality.

Yet, we don't have a consistent and broadly applicable set of measures that provides a common reference point for further analysis and collaboration.

In the United States, the PCAOB plans to issue a concept release in the very near future to help advance a discussion about potential indicators of audit quality.

In my view, a key component of the future evolution in independent audit regulation is to find common approaches to measure and candidly discuss the state of audit quality.

This will facilitate more consistent and effective audit regulation for the protection and benefit of investors.

At this point, I would like to turn the program over to our first speaker on this morning's introductory session on the PCAOB, Mr. Gordon Seymour, the PCAOB's General Counsel.

Gordon will provide you with an overview of the PCAOB and its operations.

Thank you and enjoy the Institute.

Net Neutrality: President Obama's Plan for a Free and Open Internet

More than any other invention of our time, the Internet has unlocked possibilities we could just barely imagine a generation ago.

And here's a big reason we've seen such incredible growth and innovation: Most Internet providers have treated Internet traffic equally.

That's a principle known as "net neutrality" — and it says that an entrepreneur's fledgling company should have the same chance to succeed as established corporations, and that access to a high school student's blog shouldn't be unfairly slowed down to make way for advertisers with more money.

That's what President Obama believes, and what he means when he says there should be no gatekeepers between you and your favorite online sites and services.

And as the Federal Communications Commission (FCC) considers new rules for how to safeguard competition and user choice, we cannot take that principle of net neutrality for granted.

Ensuring a free and open Internet is the only way we can preserve the Internet's power to connect our world. That's why the President has laid out a plan to do it, and is asking the FCC to implement it.

The President's Statement

An open Internet is essential to the American economy, and increasingly to our very way of life.

By lowering the cost of launching a new idea, igniting new political movements, and bringing communities closer together, it has been one of the most significant democratizing influences the world has ever known.

“Net neutrality” has been built into the fabric of the Internet since its creation — but it is also a principle that we cannot take for granted.
We cannot allow Internet service providers (ISPs) to restrict the best access or to pick winners and losers in the online marketplace for services and ideas.

That is why today, I am asking the Federal Communications Commission (FCC) to answer the call of almost 4 million public comments, and implement the strongest possible rules to protect net neutrality.

When I was a candidate for this office, I made clear my commitment to a free and open Internet, and my commitment remains as strong as ever.

Four years ago, the FCC tried to implement rules that would protect net neutrality with little to no impact on the telecommunications companies that make important investments in our economy.

After the rules were challenged, the court reviewing the rules agreed with the FCC that net neutrality was essential for preserving an environment that encourages new investment in the network, new online services and content, and everything else that makes up the Internet as we now know it.

Unfortunately, the court ultimately struck down the rules — not because it disagreed with the need to protect net neutrality, but because it believed the FCC had taken the wrong legal approach.

The FCC is an independent agency, and ultimately this decision is theirs alone.

I believe the FCC should create a new set of rules protecting net neutrality and ensuring that neither the cable company nor the phone company will be able to act as a gatekeeper, restricting what you can do or see online.

The rules I am asking for are simple, common-sense steps that reflect the Internet you and I use every day, and that some ISPs already observe.

These bright-line rules include:

No blocking. If a consumer requests access to a website or service, and the content is legal, your ISP should not be permitted to block it.

That way, every player — not just those commercially affiliated with an ISP — gets a fair shot at your business.

No throttling. Nor should ISPs be able to intentionally slow down some content or speed up others — through a process often called “throttling” — based on the type of service or your ISP’s preferences.

Increased transparency. The connection between consumers and ISPs — the so-called "last mile" — is not the only place some sites might get special treatment.

So, I am also asking the FCC to make full use of the transparency authorities the court recently upheld, and if necessary to apply net neutrality rules to points of interconnection between the ISP and the rest of the Internet.

No paid prioritization. Simply put: No service should be stuck in a "slow lane" because it does not pay a fee.

That kind of gatekeeping would undermine the level playing field essential to the Internet's growth.

So, as I have before, I am asking for an explicit ban on paid prioritization and any other restriction that has a similar effect.

If carefully designed, these rules should not create any undue burden for ISPs, and can have clear, monitored exceptions for reasonable network management and for specialized services such as dedicated, mission-critical networks serving a hospital.

But combined, these rules mean everything for preserving the Internet's openness.

The rules also have to reflect the way people use the Internet today, which increasingly means on a mobile device.

I believe the FCC should make these rules fully applicable to mobile broadband as well, while recognizing the special challenges that come with managing wireless networks.

To be current, these rules must also build on the lessons of the past.

For almost a century, our law has recognized that companies who connect you to the world have special obligations not to exploit the monopoly they enjoy over access in and out of your home or business.

That is why a phone call from a customer of one phone company can reliably reach a customer of a different one, and why you will not be penalized solely for calling someone who is using another provider.

It is common sense that the same philosophy should guide any service that is based on the transmission of information — whether a phone call, or a packet of data.

So the time has come for the FCC to recognize that broadband service is of the same importance and must carry the same obligations as so many of the other vital services do.

To do that, I believe the FCC should reclassify consumer broadband service under Title II of the Telecommunications Act — while at the same time forbearing from rate regulation and other provisions less relevant to broadband services.

This is a basic acknowledgment of the services ISPs provide to American homes and businesses, and the straightforward obligations necessary to ensure the network works for everyone — not just one or two companies.

Investment in wired and wireless networks has supported jobs and made America the center of a vibrant ecosystem of digital devices, apps, and platforms that fuel growth and expand opportunity.

Importantly, network investment remained strong under the previous net neutrality regime, before it was struck down by the court; in fact, the court agreed that protecting net neutrality helps foster more investment and innovation.

If the FCC appropriately forbears from the Title II regulations that are not needed to implement the principles above — principles that most ISPs have followed for years — it will help ensure new rules are consistent with incentives for further investment in the infrastructure of the Internet.

The Internet has been one of the greatest gifts our economy — and our society — has ever known.

The FCC was chartered to promote competition, innovation, and investment in our networks.

In service of that mission, there is no higher calling than protecting an open, accessible, and free Internet.
I thank the Commissioners for having served this cause with distinction and integrity, and I respectfully ask them to adopt the policies I have outlined here, to preserve this technology's promise for today, and future generations to come.

Remarks to the American Bar Association's Business Law Section Fall Meeting - Andrew Ceresney Director, SEC Division of Enforcement Washington D.C.

SEC Headquarters, Washington, DC

Before I begin, let me give the requisite reminder that the views I express today are my own and do not necessarily represent the views of the Commission or its staff.

I am pleased to be here this morning to talk about the latest developments in the SEC's Enforcement Division.

The SEC recently completed its fiscal year, which was my first full fiscal year as Enforcement Director and Chair White's first as Chair.

As a result, I wanted to spend a little time today highlighting some of our successes over the past year, look briefly at what to expect in the coming year, and then talk about some areas that have been the focus of much discussion in recent months — administrative proceedings, admissions, and our increased use of big data.

Record Year in Enforcement

Let me begin by providing a brief recap of the Division's accomplishments over the last year. By any measure, Enforcement had a banner year last year.

We filed ground-breaking cases that impacted every corner of the industry — from market structure to financial reporting, asset management to insider trading, municipal securities, FCPA, and more — and we obtained significant monetary penalties and other relief.

In total, we filed 755 actions last year — the most ever filed in the history of the Commission.

And we obtained orders for over $4 billion in monetary sanctions — nearly 20% larger than our previous high.

But as I always say, numbers only tell a small part of the story.
What made our year particularly noteworthy was the breadth and impact of our actions.

And the violations we pursued — large and small — sent important messages to the market, protected investors, and served as a strong deterrent to would-be violators.

Last year, for example, we brought a number of first-of-their-kind actions, including our first series of cases involving violations of the market access rule; our first action enforcing the "pay to play" rule for investment advisers; our first action against a private equity firm relating to its allocation of fees and expenses; and our first case charging violations of the whistleblower anti-retaliation provisions.

We also announced a whistleblower award of over $30 million, our largest ever, to someone who provided key, original information that led to a successful enforcement action.

As our year-end numbers indicate, we also used our penalty authority more aggressively last year, including a $16 million penalty for net capital violations — the largest ever imposed for such misconduct by a factor of 40; the largest penalty to date against an alternative trading system; and the largest penalties ever assessed against individuals in an FCPA case.

We brought significant actions against financial institutions last year, including cases related to misconduct dating back to the financial crisis and cases involving serious failures in controls.

We also made progress this past year in our efforts to combat microcap fraud, bringing impactful cases and using our temporary suspension authority much more frequently to cut off pumps before they turned into dumps.

And we brought a number of cases involving pyramid schemes that targeted low income and minority communities, a trend we are seeing more and more.

We saw our numbers of financial reporting cases rise by almost one-half as we increased our focus on this area.

We also continued to bring significant insider trading cases — charging 80 people this past year, including industry insiders, husbands who traded on information they learned from their wives, and a group of golfing buddies and other friends.

Our Successful Litigation and Trial Record

The most recent fiscal year also was a banner year for our litigation program, including trial victories, summary judgment wins, the imposition of robust remedies, and positive decisions from federal appellate courts.

We tried more cases in federal court this past year than in any of the previous 10 years.

And we tried more cases to juries this year than in the three previous years combined.

Overall, we had 30 trials this past year. That is a big number for us, almost twice the number as the prior year.

Our trial results are consistently strong over time — we win around 80 percent of our trials — and this year we scored a series of strong wins in challenging cases of all stripes against experienced defense counsel.

In fact, we have prevailed in our last ten jury trials and administrative proceedings, for example.

Key trial wins include two recent jury trial victories by our Boston and Fort Worth offices over investment advisors Charles Kokesh, for defrauding his firm's advisory clients by systematically looting around $35 million in client funds over many years, and Lee Benjamin Grant, for misleading his brokerage customers into transferring their assets to Grant's new advisory firm.

And our Home Office prevailed before a jury in an epic fraud case against the Wyly brothers — Texas billionaires who hid hundreds of millions of dollars in an elaborate offshore trust system and used the trusts to secretly profit in companies they controlled.

Even as we prevail consistently at trial, I am reminded that the cases we try in court are the toughest securities cases around.

Our strongest cases typically go criminal or settle, or we prevail on summary judgment.

I understand, therefore, that we won't win all of our cases.

What is important to me is that we aggressively bring impactful cases and put our strongest case forward in court, and that is what we have been doing.

And we are not just winning at trial and on summary judgment — we also are helping investors by winning strong remedies that help compensate victims and protect the investing public.

In the Wyly trial, for example, the judge issued a preliminary decision requiring Sam Wyly and Charles Wyly's estate to pay disgorgement of approximately $187 million, and our total relief is expected to rise to $300 million or even more.

We also recently secured an asset freeze against the defendants and their family members to help make sure the anticipated judgment gets paid.

We also are seeing a maturation of our cooperation program.

This past year included our first litigated action that featured a testifying SEC cooperator — the Gonnella case, in which we prevailed last week in an administrative hearing — as well as other actions where cooperators played key roles in positive outcomes, including our first-ever non-prosecution agreement for an individual who provided early, extraordinary and unconditional cooperation that led to findings of liability against multiple tippers and insider traders.

The Year Ahead

So this past year was an outstanding year. But of course, we are now looking forward and our pipeline of cases is as strong as ever.

I expect significant cases in all aspects of our program in the next year, including significant market structure cases against exchanges, ATSs and broker-dealers; important financial reporting and audit cases, including fraud cases, cases against auditors, and violations of the internal controls requirements; insider trading cases against traders of all different types; microcap fraud cases against repeat players, including promoters who have spearheaded many schemes and attorneys who have facilitated them; FCPA cases involving unique facts, using the broad definition of "anything of value"; asset management cases, including misrepresentations of fund performance and failures to disclose conflicts of interest; important cases relating to complex products and credit ratings from our Complex Financial Instruments Unit; and more ground-breaking cases in the muni

markets, expanding our reach to new areas and bringing cases under our MCDC initiative.

Administrative and Cease-and-Desist Proceedings

I wanted to spend a bit of time speaking about our use of the administrative forum, which has been a frequent topic of discussion at forums like this in recent months.

Let me begin with some basics about our use of the administrative forum. Contrary to the impression some may have, we have been using administrative proceedings throughout the 42-year history of the Division of Enforcement, and the Commission used them even before its enforcement activities were consolidated in one division.

SEC administrative law judges (ALJs) have adjudicated hundreds of enforcement matters over the years.

Many of these cases were against regulated entities and individuals, and involved extensive factual records, complex and novel legal issues, and claims for significant financial penalties.

So ALJs have been presiding over and adjudicating complex securities cases for decades.

Until 2010, while we could proceed against unregistered persons in administrative proceedings, the relief that we could obtain against them was limited.

In the Dodd-Frank Act, however, Congress provided us authority to obtain penalties in administrative proceedings against unregistered parties comparable to those we already could obtain from registered persons.

Before that, penalties against unregulated entities or individuals were only available in district court.

That legislative change allows us to obtain many — though not all — of the same remedies in administrative proceedings as we could get in district court.

And so what we are doing now is simply making use of the administrative forum in cases where we previously could only obtain penalties in district court.

This change, however, does not mean that we will choose the administrative forum in every case.

For settled matters, we often, but not always, choose to file in an administrative forum, largely because of efficiency.

The filing quickly ends the matter on a settled basis, among parties that have agreed to a settlement, and there is no need to have implementation of the parties' agreement subject to the competing demands of busy district court dockets.

This practice was recently endorsed by the Second Circuit Court of Appeals in the Citi decision, where the court noted that the Commission "is free . . . to employ its own arsenal of remedies" rather than bring settlements to district court.

As for litigated cases, we evaluate each case to determine the appropriate forum based on the facts and circumstances.

There is no question that we are using the administrative forum more often now than in past years, given the changes under Dodd-Frank.

Contrary to the notion some have that we are running away from cases in district court, however, if you look at actions we filed last year on at least a partially litigated basis, approximately 57 percent were filed in district court, and around 43 percent were filed in the administrative forum.

So we clearly are not shunning federal court in our litigated actions.

There are a number of benefits to using the administrative forum that can lead us to file cases there.

First, administrative actions produce prompt decisions.

An ALJ normally has 300 days from when a matter is instituted to issue an initial decision.

That deadline can be extended in certain cases, but the hearings are still held promptly.

For cases we file in district court, we can often go 300 days and still be just at the motion to dismiss stage or part of the way through discovery, with any trial still far down the road.

Proof at trial rarely gets better for either side with age; memories fade and the evidence becomes stale.

And from the standpoint of deterrence and investor protection, I think we can all agree that it is better to have rulings earlier rather than later.

Doing so allows us to have timely public findings of fact and law, and where we are successful, to obtain remedies like industry bars more promptly.

Second, administrative proceedings have the benefit of specialized factfinders.

The ALJs are focused on hearing and deciding securities cases, year after year.

They develop expert knowledge of the securities laws, and the types of entities, instruments, and practices that frequently appear in our cases.

Many of our cases involve somewhat technical provisions of the securities laws, and ALJs become knowledgeable about these provisions.

Third, the rules governing administrative hearings provide that ALJs should consider relevant evidence.

In practice, what this means is that ALJs are guided by, but not obligated to strictly apply, the Federal Rules of Evidence.

They are free to give each piece of evidence the weight that they deem appropriate.

Finally, certain types of charges, such as failure to supervise or "causing" violations, can be brought only in the administrative forum.

I should note that these features of the administrative forum can also benefit the respondents.

Either side can benefit when witnesses' recollections are fresher.

And the relaxed rules of evidence may likewise give them more flexibility in offering evidence.

With all this said, there are situations where district court is the more appropriate forum.

In certain cases, we need certain types of discovery that we can only get in district court.

For example, where we file our case on an expedited basis to stop an ongoing fraud, a district court might be the only option that allows us to act quickly while still being able to gather evidence.

In certain cases, we need emergency relief, such as an asset freeze or receiver, and that requires an order from a district court.

We also may believe that we can obtain summary judgment in district court.

The bottom line is that we make a case by case determination of which forum is appropriate based on the particular facts of the case.

Now there has been some criticism recently of our use of administrative proceedings against unregistered entities and individuals and suggestions that these proceedings are unfair.

I reject that assertion.

ALJs call it like they see it, and I note that we have lost some significant proceedings before ALJs in the last few years.

Further, I would challenge anyone to identify a case in which an ALJ erroneously ruled for us where the Commission did not reverse the decision.

Some have raised concerns about the lack of a jury in administrative hearings.

But the Supreme Court has considered and rejected the argument that there is a Constitutional right to a jury trial for government claims based on statutes like the federal securities laws.

Some also have claimed that the procedural rules that govern administrative proceedings, including the time frames for the hearings and the rarity of depositions, are unfair to respondents. Some have even suggested they create a due process concern.

Of course, as I suggested previously, we have been using this forum for years in complicated proceedings involving registered parties and no due

process violation has been found in those cases. But in any event, the rules for administrative proceedings provide extensive procedural protections.

These rules require us to commence making available our entire investigative file within seven days of the filing of our allegations, and we typically provide the whole file in that time frame.

We also have affirmative Brady obligations to disclose material, exculpatory information and Jencks Act obligations to turn over statements of our witnesses — neither of which apply in our district court proceedings. ALJs commonly require us to provide our witness lists and exhibit lists well in advance of the hearing, putting respondents on further notice about the specific content of our case.

A respondent and the Division both have the right to request third-party subpoenas for witnesses and documents.

And apart from all of the information we turn over, it also is worth noting that in many cases respondents know full well what the important evidence is, either because they produced it to us themselves, because it was testimony from their own employees or someone else to whom they have access before the hearing, or because we have shared it with them in testimony or in the course of Wells discussions.

So the bottom line is that there are extensive procedural protections in our proceedings and defendants have transparency into the nature of our case and proof well before the hearing commences.

It is true that there generally are no depositions under the administrative Rules of Practice. But I do not think that due process requires the ability to conduct depositions.

In a former life, I was a criminal prosecutor, and I saw many people sentenced to prison without any chance of deposing the government's witnesses before trial.

The Federal Rules of Criminal Procedure allow for depositions only in "exceptional circumstances," which is similar to what the Commission's Rules of Practice allow.

If that approach is acceptable where someone's liberty is on the line, then it is hard to see how due process requires more for respondents in administrative proceedings.

Some have raised the concern that the use of administrative proceedings will impair the proper development of the law by district court judges.

But using the administrative forum furthers the balanced and informed development of the federal securities laws, just as it does in other specialized legal areas in which administrative agencies function.

SEC commissioners have great expertise in the securities laws and the administrative agency structure that Congress created leverages that expertise to help shape the law's development.

The commissioners review ALJ decisions de novo.

The parties have the right to appeal an adverse Commission decision to a circuit court, where panels of federal judges may have the final say on the development of the law.

So the Commission has input on important questions, but legal rulings either supporting or reversing the Commission frequently are made at the circuit or Supreme Court level.

I also would note that two seminal insider trading cases, Cady Roberts and Dirks, followed that path, starting in the SEC's administrative forum and, in the case of Dirks, ending up in the Supreme Court.

So this process has worked well over the years in developing the securities laws.

My bottom line is that, while we are using administrative proceedings more, we are still bringing significant numbers of contested cases in district courts.

And our use of the administrative forum is eminently proper, appropriate, and fair to respondents.

Admissions

Of course, the changes within our enforcement program extend beyond our increased use of administrative proceedings.

As many of you no doubt are aware, we modified the Commission's longstanding no-admit, no-deny settlement protocol by considering

requiring admissions in certain types of cases where heightened accountability and acceptance of responsibility are in the public interest.

The practice of primarily settling our cases on a no admit/no deny basis has served the SEC — and other agencies — well for many years.

These settlements speed up our ability to return funds to wronged investors, avoid the delay and uncertainty inherent in trials, and allow us to use our finite resources more effectively.

As I noted, earlier this year, the Second Circuit reaffirmed the significant deference accorded to the Commission in determining on what terms to settle with parties.

For these reasons, settlements without admissions have been — and will continue to be — an important part of our enforcement regime.

That being said, a little over a year ago, Chair White announced a change in our settlement approach by which we would consider requiring admissions in certain categories of cases where there is a greater need for public accountability.

Her years in the United States Attorney's Office for the Southern District of New York taught her — and me — the power and importance of defendants admitting that they broke the law.

As you probably know, in the criminal realm, all guilty pleas are accompanied by factual admissions, which eliminate any doubt about the defendant's conduct and provide additional accountability for the crime.

I am happy to report that the program is working well as we have obtained admissions in over a dozen cases under the new policy.

The Wedbush settlement announced yesterday is just the latest, and more are in the pipeline.

These admissions have come from a broad range of defendants — firms and individuals, as well as regulated and unregulated entities — and involve a broad range of conduct that includes both scienter and non-scienter-based violations.

And each successive case where we obtain admissions has helped illuminate the circumstances in which we will conclude that they are appropriate.

Admissions will be considered in certain types of cases, including those involving egregious conduct, where large numbers of investors were harmed, where the markets or investors were placed at significant risk, where the wrongdoer posed a particular future threat to investors or the markets, where the defendant engaged in unlawful obstruction of the Commission's processes, or where admissions would significantly enhance the deterrence message of the action.

And our admissions cases to date have touched on each of these respective categories.

Overall, I think there is no serious question that our new approach to admissions has strengthened our enforcement program and ensured greater public accountability, and has provided us with another important tool in punishing and deterring misconduct.

Using Big Data

Finally, I want to say a few words about another important trend in our enforcement efforts — our use of big data to detect and investigate violations.

The Division and the agency as a whole have made great strides in leveraging data and technology to enhance our ability to detect and pursue misconduct.

With the proliferation of big data, and growing complexity of our markets, we need to better harness technology in order to keep up with wrongdoers. So we are developing new analytic tools designed to process data more efficiently.

Let me give some examples.

A key development for us in connection with our insider trading efforts is our use of new analytical tools to increase our capability of detecting insider trading.

We have developed sophisticated tools that allow us to detect parties trading in unison, which then enables us to work our way back to the source of the inside information.

A number of cases we have brought this year were built using this sort of data analytics, and we have numerous additional investigations in the pipeline that originated from these tools.

We are doing similar things in many other areas as well.

Our Financial Reporting and Audit Task Force is using technology in a number of ways.

It is working closely with the Division of Economic and Risk Analysis, for example, to refine a tool they developed that compiles public company filing data, compares it with results of other companies in the same industry, and detects anomalous results that might call for further investigation.

We also are sifting through non-public clearing firm data for problematic patterns in the sale and trading of certain asset-backed securities and other complex products.

Through this process, we are deploying proprietary data analytics to identify troubling trends in the sale of complex financial instruments to retail investors that might serve as the basis of a suitability or failure-to-supervise case.

Finally, our Broker-Dealer Task Force has developed initiatives utilizing technology and data-driven analysis to target excessive trading in customers' accounts and inadequate compliance with the anti-money laundering and Bank Secrecy Act regulations.

Through these efforts, we are becoming more effective and efficient at uncovering and pursuing misconduct, and improving our ability to keep pace with our rapidly transforming markets.

Conclusion

I'm going to end here, but not because I'm out of things to say about the exciting work going on throughout the Division of Enforcement.

Far from it.

I suspect that many of you in this room could attest to the fact that we are moving forward in cutting-edge investigations across the full span of the industry.

This is why our most recent fiscal year was such a success, and why I'm confident that there are many more great things to come.

Thank you for your attention, and enjoy the rest of this conference.

Improving financial institution supervision - examining and addressing regulatory capture

Testimony by Mr William C Dudley, President and Chief Executive Officer of the Federal Reserve Bank of New York, before the Senate Committee on Banking, Housing, and Urban Affairs Financial Institutions and Consumer Protection Subcommittee, Washington DC

I. Introduction

Chairman Brown, Ranking Member Toomey, and members of the Subcommittee, thank you for this opportunity to testify on the effectiveness of financial institution supervision and the issue of regulatory capture.

In 2008 and 2009 our country faced its worst financial crisis since the Great Depression.

I mention those years as a touchstone for my remarks today.

Despite the passage of time and an economy that is steadily improving, the financial crisis is hardly something that happened in the remote past.

For the too many people who are still unemployed or underemployed, or who otherwise continue to struggle financially, it is living history.

While the causes of the crisis remain subject to debate, it is undeniable that banking supervisors could have done better in their prudential oversight of the financial system.

This conclusion raises two fundamental questions:

- First, how can we improve the stability of the financial system? In other words, how can we make the financial system more resilient and productive?

- Second, how can we improve our supervision of financial institutions?

The Federal Reserve is working diligently to improve both stability and supervision.

The two concepts are linked.

Since the financial crisis, the Federal Reserve has made significant changes to the substance and process of supervision.

As a result, the financial system is unquestionably much stronger and much more stable now than it was five years ago.

II. Substantive changes

Since the financial crisis, the Federal Reserve has redoubled its attention to bank capital.

Capital is the financial cushion that banks hold to absorb loss.

It provides an economic firebreak that helps prevent systemic stress from turning into a full-blown crisis.

Before the crisis, capital requirements were too low and inconsistent across jurisdictions.

Moreover, too much of the capital held by banks was of poor quality, and their internal capital assessments were not forward-looking.

Since the crisis, new regulation and heightened supervision have increased both the quantity and the quality of equity capital at the largest financial institutions that we regulate and supervise.

The Federal Reserve and other federal banking regulators implemented so-called "Basel III" international capital standards in July 2013, which raised the minimum ratio of common equity Tier 1 capital to risk-weighted assets.

Federal regulation also now requires stricter criteria for instruments to qualify as regulatory capital and higher risk weights for many classes of assets.

And the Federal Reserve mandated a new minimum supplementary leverage ratio that includes off-balance sheet exposures for the largest, most internationally active banking organizations and a leverage surcharge for large U.S. banking organizations.

In support of these new regulations, capital assessment has become a focus of supervision since the financial crisis.

Examiners monitor capital reserves and put banks through periodic stress tests that are evaluated on a cross-firm basis.

This has been one of the great advancements of bank oversight following the crisis.

These evaluations enable supervisors to assemble a composite assessment of the nation's banking sector, which materially assists the Federal Reserve in its statutory mandate to promote financial stability.

The Dodd-Frank Act mandates supervisory stress tests that assess whether large bank holding companies have a sufficient level of capital to absorb losses during adverse economic conditions.

The Federal Reserve also conducts a capital planning exercise, called the Comprehensive Capital Analysis and Review or "CCAR."

This evaluation combines the quantitative results from the Dodd-Frank Act stress tests with a qualitative assessment of whether the largest bank holding companies have vigorous, "forward-looking capital planning processes that account for their unique risks."

The criteria for both sets of stress tests are dynamic and change in response to evolving risks.

For example, past tests have assumed a sharp, sudden, and widespread drop in markets triggered by, say, a large Eurozone shock.

The tests also evaluate market interconnectedness, including the risk of major counterparty default.

To increase public transparency, the Federal Reserve now publishes the overall results of its stress tests.

This helps rebuild confidence in the strength of the financial system.

The most recent round of stress tests concluded in the first quarter of this year.

In my view, the results were encouraging, although not uniformly satisfying.

In general, "firms participating in CCAR have more than doubled their Tier 1 common capital since 2009, an increase of $500 billion of additional, high-quality capital in the U.S. financial system."

This impressive statistic notwithstanding, the Federal Reserve objected to capital plans from five of the 30 participating firms.

Four of those five firms submitted plans that raised firm-specific, qualitative concerns.

The remaining firm failed to meet a minimum quantitative requirement.

The consequences of failing to pass a stress test can be severe.

If its capital plan has been rejected, the Federal Reserve may, among other things, restrict a bank holding company from paying or increasing dividends on its common stock or increasing any repurchase of its common stock, or both.

For example, as a result of this year's CCAR, Citigroup was not permitted to begin a new common stock repurchase program or to increase its quarterly common stock dividend.

As a companion to improved capital, the Federal Reserve also assesses liquidity - that is, how quickly a bank can convert its assets into cash.

Prior to the crisis, liquidity practices did not generally anticipate the possibility of severe drops in the prices of saleable assets.

Following the crisis, the Federal Reserve imposed new liquidity regulations, including the Basel III Liquidity Coverage Ratio.

The objective of these new regulations is to require large firms to hold levels of liquid assets sufficient to protect against constraints on their funding during times of financial turmoil.

We have also implemented liquidity stress test assessments for systemically important financial institutions.

These assessments provide important insight into the adequacy of liquidity positions and bank preparedness for upcoming regulatory standards.

Beyond capital and liquidity, the Federal Reserve has increased its focus on risk management practices at the largest and most systemically important financial institutions.

We learned from the crisis that risk management in the financial services industry had not always kept pace with changing market practices.

We have responded in several ways.

For example, we have paid greater supervisory attention to corporate governance.

We significantly increased the depth and frequency of interaction between senior supervisors from the Federal Reserve and directors and executives at banks.

This supplements our ongoing assessment of management's oversight of risk.

Our review entails a critical analysis not only of firm policies, procedures and limits, but also of the quality of the risk reports escalated to senior management, the capabilities of the firm's risk monitoring program, and the adequacy of control functions.

We have also increased our enforcement activity for violations of law or unsafe or unsound conduct.

Since 2009 the Federal Reserve has taken 36 public enforcement actions against institutions supervised by the New York Fed, which included $1.2 billion in fines.

On top of this, five firms supervised by the New York Fed paid $1.3 billion into a qualified settlement fund for mortgage borrowers, and the same five institutions were required to provide over $2 billion in other foreclosure prevention assistance.

These statistics do not include non-public enforcement actions, including restrictions on the further growth of banks that do not have satisfactory risk management regimes.

And, earlier this year, we assisted in consigning the concept of "too big to jail" to history when Credit Suisse and BNP Paribas pleaded guilty to criminal charges.

I am gratified that the Attorney General and the United States Attorney for the Southern District of New York have acknowledged the work of the Federal Reserve in supporting our law enforcement partners.

The New York Fed has also devoted significant resources and attention to the reform of bank culture and conduct.

Increased capital and liquidity are important tools to promote financial stability, but in the end a bank is only as trustworthy as the people who work within it.

I have personally delivered a strong message that the culture of Wall Street is unacceptable.

Bad conduct by bankers damages the public trust placed in banks. In my view, this loss of trust is so severe that it has become a financial stability concern.

If bad behavior persists, it would not be unreasonable - and may even be inevitable - for one to conclude that large firms are too big and complex to manage effectively.

Our nation's largest financial institutions need to repair the loss of public trust in banks.

This means a back-to-basics assessment of the purpose of banking, including duties owed to the public in exchange for the privileges banks receive through their bank charters and other functions of law.

Among these privileges are deposit insurance and access to a lender of last resort.

As part of this effort, I have proposed four specific reforms to curb incentives for illegal and unduly risky conduct at banks.

First, banks should extend the deferral period for compensation to match the timeframe for legal liabilities to materialize - perhaps as long as a decade.

Second, banks should create de facto performance bonds wherein deferred compensation for senior managers and material risk takers could be used to satisfy fines against the firm for banker misbehavior.

Third, I have urged Congress to enact new federal legislation creating a database that tracks employees dismissed for illegal or unethical behavior.

Fourth, I have requested that Congress amend the Federal Deposit Insurance Act to impose a mandatory ban from the financial system - that is, both the regulated and shadow banking sectors - for any person convicted of a crime of dishonesty while employed at a financial institution.

III. Supervisory process

In tandem with our attention to capital, liquidity, and risk management, we have made important changes to the process of supervision.

For starters, the Federal Reserve now makes its most consequential supervisory decisions on a system-wide level through the Large Institution Supervision Coordinating Committee or "LISCC."

The committee comprises representatives across professional disciplines from several Reserve Banks and the Board of Governors.

The New York Fed supplies only three of its 16 members.

LISCC sets supervisory policy for the 15 largest, most systemically important financial institutions in our country and develops innovative, objective, and quantitative methods for assessing these firms on a comparative basis.

LISCC also coordinates the supervision of the largest supervised institutions through its Operating Committee, which reviews and approves supervisory plans for exams, receives regular updates on major supervisory issues, and makes material supervisory decisions regarding matters that affect the firms' safety and soundness.

In this respect, the Operating Committee provides an important safeguard against regulatory capture by ensuring that no one person or Reserve Bank has the power to make a final decision on a matter of significance.

Another procedural change is our increased application of cross-firm, horizontal review.

This technique enables peer-to-peer comparison of banks, facilitates a better assessment of the overall health of the financial system, and

safeguards against regulatory capture by providing insight from across the Federal Reserve System.

The analysis is done not only at the level of the Board of Governors - for example, through CCAR and Dodd-Frank stress testing - but also within the New York Fed.

We hold weekly discussions among senior supervisory and risk officers to identify developing concerns that may pose a systemic risk.

A current subject of horizontal analysis is leveraged loans - specifically, whether lax underwriting practices for such loans could pose a significant risk to financial stability.

In addition, we have reorganized the supervision group at the New York Fed in a number of ways that promote unbiased analysis and professional objectivity.

Many of these changes directly reflect the recommendations in a 2009 report that I commissioned from David Beim, which was featured in the recent This American Life program about supervision at the New York Fed.

For example:

- Over the last five years, we have reassigned some of our most senior personnel to front-line positions at the largest supervised institutions.

We also recruited experienced executives with financial backgrounds from outside the New York Fed.

The purpose of these personnel changes was to position leaders with the confidence and depth of professional experience necessary to challenge the leadership of supervised financial institutions.

- We increased training, especially for more senior examiners.

Since 2011, we have required enhanced training for senior supervisory officers on corporate governance, business strategies, and risks.

Our goal is to deliver stronger and clearer supervisory views to boards of directors and senior management.
Also since that year, we have offered a customized management development program for managers in the supervision group.

- We hired more risk specialists and created the role of business-line specialist to assess the risks and vulnerabilities in firms' business models.

- We continue to require that examiners rotate to another institution after three to five years.

This tenure allows enough time to gain an understanding of a firm without sacrificing examiner independence.

- We have taken concrete steps to encourage examiners to speak up, which we view as a core competency.

For example, we evaluate examiners on their level of engagement with colleagues and their willingness to share insights.

- We created programs to encourage peer recognition of good ideas, including funding for new supervision ideas proposed and voted on by supervisory staff.

- We increased the opportunities for feedback to senior managers, including the head of supervision, in addition to other channels already provided by the New York Fed.

Among other improvements, we conduct regular town halls and provide a standing, on-line forum as a device to funnel questions to group leaders.

In both settings, questions and answers are offered in an open, transparent manner.

- And we require examination teams to spend more time at New York Fed headquarters and less time "in the field."

Additional time at headquarters promotes cross-firm discussion and direct communication between senior managers and examiners.

For example, we offer a seminar series at which group leaders discuss key issues in supervision with our supervision staff.

Each and together, these improvements to the substance and process of supervision contribute to financial stability by providing greater insight into bank resiliency and risk.

But these enhancements are not self-executing.

They depend on the hundreds of examiners who are dedicated professionals working in the public interest.

Our examiners fulfill their obligations with considerable care, mindful of the stakes to Main Street when something goes wrong on Wall Street.

I am grateful for their efforts.

IV. Reasonable expectations

Before concluding, let me offer a broader view of what we at the Federal Reserve expect from prudential supervision. Very briefly, I submit that supervision should be fair, conscientious, and effective.

Fair supervision means that the rules are applied consistently across the firms we supervise.

We all need to know the rules and follow the same rule book.

It also entails a commitment to independence from business or political influence, as envisioned by the Federal Reserve Act one hundred years ago.

Conscientious supervision means we must be committed to sustained and, if necessary, radical self-improvement.

The Beim report is an example of our willingness to commission and accept self-critical analysis and our commitment to improve.

But we cannot stop there.

To this end, we will be working with the Board of Governors on its upcoming review of whether the LISCC Operating Committee receives information that is sufficient to reach sound supervisory decisions.

One subset of this system-wide inquiry will analyze regulatory capture - specifically, how divergent views are presented to decision makers at the Board.

The review is expected to take several months.

Effective supervision means tough supervision and demands a focus on large banks that pose systemic risk.

Bank supervisors cannot prevent all fraud or illegal conduct or forestall all undesirable behavior in large, complex financial institutions.

But we can help create more resilient, less complex, and better managed organizations that promote, rather than undermine, financial stability.

V. Conclusion

The Federal Reserve will continue to improve its supervision and regulation of financial institutions. We understand the risks of doing our job poorly and of becoming too close to the firms we supervise.

We work hard to avoid these risks and to be as fair, conscientious, and effective as possible.

Of course, we are not perfect. We cannot catch or correct every error by a financial institution, and we sometimes make mistakes.

But in my view, a good measure of the effectiveness of supervision is the improved strength and stability of banks since the financial crisis.

Thanks in part to enhanced supervision and regulation, banks "have the ability to meet their financial obligations and continue to make a broad variety of financial products and services available to households and businesses even in times of economic difficulty."

I can promise you that we will always strive to improve and that we will work hard to earn and retain your trust.

I look forward to taking questions.

Conference on Current Issues in Securities Regulation: The 'Hot' Topics

Keynote Address at Columbia Law School Commissioner Kara M. Stein

Thank you, John [Coffee], for your kind introduction.

Before I begin my remarks, I am required to tell you that the views I am expressing today are my own and do not necessarily reflect those of the Commission, my fellow Commissioners, or the staff of the Commission.

It is a pleasure to speak in front of an audience that cares so passionately about securities regulation.

You are taking the time to think about what is and is not working in our securities laws.

And, more importantly, you are thinking about possible solutions to make our laws work better.

The issues that you are discussing today are all important.

There are panels on money market funds, dark pools, and high frequency trading.

As aptly noted by the name of the conference, these certainly are some of the "hot" topics in securities regulation.

They present complicated issues. And while each topic has its own intricacies, all of them would benefit from greater transparency.

That's why today I thought I would start out by talking about the importance of transparency in our securities markets.

Then, I'll talk about two areas where the Commission has recently enhanced transparency: the municipal securities market and the private equity market.

I will conclude with some thoughts on exchange traded funds (ETFs) and the broader market impacts of new structures that seek to relax the transparency requirements for these funds.

The Importance of Transparency

Transparency has long been central to effective securities regulation. While it's not the only tool the Commission has in its toolbox, it's foundational.

Felix Frankfurter, one of the principal drafters of the Securities Act of 1933, was a notable disciple of transparency, as was reform advocate Louis Brandeis.

As Brandeis famously said, "Publicity is justly commended as a remedy for social and industrial diseases.

Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."

As we've seen for 80 years at the Commission, this electric light has helped make our markets fair and efficient.

Done right, it enables us to be confident that in a world of competitive pressures and seemingly endless options, families can make smart choices and take responsibility for their own futures.

The informed decisions of our individuals, families, and institutions are one of the most efficient ways for businesses to access the capital they need to grow, prosper, and create jobs for millions of Americans; while also enabling them to benefit from the productive efforts of the businesses they invested in, so that they can save for retirement and pay for their children's educations, and more.

In no small part due to transparency, America continues to have the most vibrant securities markets in the world.

But there is still room for improvement, starting with the municipal securities market.

Transparency in the Municipal Securities Market

Municipal finance has been essential to the growth of our nation and, in particular, New York.

The first municipal bond on record in the United States was an 1812 New York offering that helped pay for the digging of a canal.

Municipal securities also funded the Croton Aqueduct, which helped meet the growing demand in New York for things that many of us take for granted, such as clean water and water to fight fires.

State and local governments, through municipal finance, continue to provide the bulk of our current infrastructure funding nationally, helping to provide roads, schools, and countless other services.

This creates jobs both in the short and long-term, gives businesses the confidence to operate, and enhances our citizens' quality of life.

In order to continue to support our nation's infrastructure, state and local governments continue to need capital. And that capital comes primarily from ordinary investors, who own over 70 percent of the market directly or through investment companies.

In recent years, there have been significant improvements in transparency in this market thanks to the work of the Municipal Securities Rulemaking Board (MSRB), which has harnessed the power of technology through its free, electronic repository of information called the Electronic Municipal Market Access system, or EMMA.

The SEC also brought new attention to this market by implementing Congress' mandate that municipal advisors — those who help our state and local governments in their financing efforts — register with the Commission.

In addition, the SEC has brought a series of enforcement actions that held issuers accountable for the disclosures that investors rely upon.

But large gaps in transparency in this market still exist.

This has significant costs to retail investors, who are unable to demand competitive transaction pricing because they lack basic information.

Calls to bring greater transparency to this market are not new. The Commission issued a 2012 report that identifies some of the ideas that I will highlight.

And several of my fellow Commissioners have expressed support for bringing more transparency to this market.

There is momentum to press ahead, and I want to discuss two areas where regulators should move forward.

The first is to provide basic post-trade pricing disclosure on customer confirmations for principal transactions.

Despite the transaction information being readily available on EMMA, investors do not receive disclosure on their confirmations showing the transaction costs that they pay when they buy or sell a municipal security in a principal transaction.

This is significant because virtually all customer transactions in this market are principal trades.

Earlier this week, the MSRB published a proposal to provide this disclosure on customer confirmations.

I encourage you to weigh in on all aspects of the MSRB proposal, as well as the related proposal by the Financial Industry Regulatory Authority (FINRA), and in particular whether the disclosure of the price differential should be a percentage of par value, a total dollar amount, or both.

While post-trade transparency is important, it is only one side of the coin.

It must be complemented with greater transparency before trading takes place.

Here, there remains a lot more work to be done.

Ordinary investors do not have the most basic of information, such as who in the market is interested in buying or selling a municipal security, and at what price.

Firm bid and ask quotes are generally unavailable, and municipal bond dealers usually do not provide firm quotations electronically.

The limited information that does exist typically is only available to institutional investors and participating dealers.

In addition, it is provided primarily through electronic networks operated by alternative trading systems (ATSs), or through municipal bond dealers that are broker's brokers.

We need to provide ordinary investors with more equal access to this information.

This should promote competition and lead to better prices for investors.

Determining the best way to do it requires deep thinking.

One option that we should explore is amending Regulation ATS to require public disclosure of pricing information.

The Commission also could require broker's brokers to publicly disclose pricing information.

If we chose this path, we will need to work through challenging issues.

For example, should such a rule apply to all electronic networks?

Should it apply to all of the transactions on the networks, or only those that exceed a threshold?

While there are no easy answers, and we must be careful to avoid unintended consequences that could lead to less transparency, these are alternatives that are worth considering given the sizeable benefits that could come from greater sunlight in this space.

Institutional Investors Need it Too — Transparency and Private Equity

Private equity, a market where most of the investors are institutions, also is benefitting from greater transparency.

Public and private pension funds, endowments, and foundations accounted for 57 percent of all investments in private equity in 2013.

This means that teachers, police officers, firefighters, and our public and private universities are relying on private equity for their financial security.

At the same time, private equity has played an increasingly important role in deploying capital to growing businesses and reforming those that are underperforming.

Many of our most promising businesses that make products that we use every day have relied on private equity.

To name just a few, private equity helped nurture and fund Microsoft, Sports Authority, and Burt's Bees.

As with the municipal securities market, in recent years there have been important advances in transparency in the private equity space.

Most investment advisers to private equity funds must now register with the Commission, and file important information regarding advisory operations and past disciplinary events.

Investors appear to appreciate the increased transparency they are receiving, and there is evidence they want more.

Investors in private equity are often sophisticated, but the range of sophistication varies.

A teacher's pension fund from a small state generally does not have the same market power, or as many employees, as a large university endowment. In addition, regardless of market power or investment acumen, it's unrealistic to expect investors to be able to replicate the access our examiners have to an adviser's records, staff, and operations.

Indeed, our Office of Compliance Inspections and Examinations (OCIE) has identified what it believes to be violations or material weaknesses in controls concerning fees and expenses in many of the exams where examiners evaluated these issues.

Now these are new registrants and a new inspection regime, and the violations may vary in severity, but these exams reveal that institutional investors too can benefit from increased transparency, as well as from the oversight that the Commission brings.

And while oversight and exams are critical, I still believe that transparency — and the investor choice and accountability that comes with it — is a much better approach as a first line of defense.

Two places where I encourage advisers to private equity funds to consider improving their own disclosures are fees that are charged to portfolio companies and performance information.

An investor's ability to understand the fees that they will be paying is one of the most important tools for evaluating any investment — and for encouraging healthy competition in the marketplace.

Unfortunately, there is evidence that fee disclosures in private equity are lacking in important ways.

For example, our exams have uncovered that some funds are separately paying "consultants" for services that they provide to portfolio companies, even though they look and act like employees of the adviser.

These "consultants" may even be described as members of the advisory team on the firm's website and in marketing materials.

Without more specific disclosure, many investors would reasonably believe that they are employees of the adviser that are being paid from the agreed upon management fee.

Our staff also has identified several cases in which investors are paying the adviser separate fees for services that the adviser provides to a portfolio company under "monitoring agreements."

These agreements often extend for long or indefinite terms that are far greater than the fund's expected holding period, and thus far beyond the time that the adviser provides services to the portfolio company.

They frequently include provisions that accelerate payments when a portfolio company is taken public or sold, resulting in fees that can amount to tens of millions of dollars or more.

The fees, however, often are not disclosed with much detail, if at all, at the time an investor commits capital to the fund.

Let me be clear.

There is nothing wrong with an investment adviser being fully compensated for services provided.

That's called getting paid to do your job! But transparency and clarity about compensation are key to making that compensation accountable and competitive.

Advisers should avoid relying on a technical interpretation of an ambiguous provision in a complex agreement to surprise investors with important information after the fund has closed.

Our markets benefit when parties clearly disclose fees to the investor before he or she makes an investment decision.

No one likes paying for something, and then getting slapped with hidden and unexpected expenses.

Not only is it fundamentally unfair, it also could undermine the health of the companies that private equity firms are supposed to help grow and thrive.

The only thing that may be more important to investors than fees is performance information, which in private equity is generally presented as an internal rate of return (IRR).

This is another area where better disclosure would be helpful.

Some advisers provide the IRR of past funds with scant detail on how it is calculated.

For example, the IRR of a fund that includes the performance of a significant number of unrealized investments that are valued by the adviser could mean something materially different to investors than an IRR based solely on realized investments.

Further, an IRR that is presented as a net return could be inflated if it includes returns on capital contributed by the fund's general partner, who typically does not pay a management fee or carried interest, or by preferred investors who pay reduced fees.

This has the potential to misrepresent performance.

I think that it is fair and reasonable to ask an adviser to clearly describe the assumptions it makes when calculating returns, and make the underlying components of the returns more transparent to all potential investors.

Simple transparency, that's what this is about.

And again, when done right, this helps make our markets competitive, allowing investors' choices to reward those who do well and hold accountable those who don't.

ETFs — A Movement to Less Transparency?

I want to turn now to some thoughts on ETFs.

Recently, the Commission has been considering novel exemptive applications for actively managed ETFs that propose to provide less transparency regarding their portfolio holdings than has been traditionally required.

While the structures that have been proposed differ, they are illustrative of the growing complexity of exchange traded products (ETPs), of which ETFs are the most popular.

The first ETFs, which began trading in 1993, sought to replicate the returns of broad-based stock market indexes such as the S&P 500.

Since then, ETFs have become significantly more complex, offering exposures across geographies, industries, currencies, commodities, and real estate.

To achieve their investment objectives, a growing, yet still small, number of ETFs employ sophisticated strategies involving options, swaps, futures, forwards, and other derivatives.

As they have become more complex, ETFs have become increasingly popular with retail and institutional investors.

Over the past decade, total net assets in ETFs have increased twelvefold, from $151 billion at the end of 2003 to $1.8 trillion at the end of June of this year.

Yet even with this impressive growth, they still comprise just slightly more than 12 percent of combined assets in registered open-end funds.

Most of the growth has been in index-based ETFs.
ETFs have not gained much of actively managed funds' market share because the Commission and its staff have traditionally required them to disclose their portfolio holdings each day.

While this has been necessary to ensure that the arbitrage mechanism works as intended, and all investors are treated equitably, it has discouraged fund sponsors from offering actively managed ETFs, because they fear that daily disclosure could allow competitors to front run their investment strategies.

The daily transparency requirement has, in effect, provided a practical ceiling on the aggregate size of ETFs.

Exchange Traded Managed Funds (ETMFs), which more closely resemble a mutual fund than an ETF, along with similar products with relaxed transparency, have the potential to break through this ceiling.

While the potential cost savings to investors are significant, ETPs raise broader questions that I have been struggling with since the "Flash Crash," when the orders of a single Kansas City trader sparked a precipitous drop in the prices and liquidity of ETFs.

If ETFs continue to grow in market share, what are the effects on our broader market structure?

For example, will it amplify volatility in the underlying securities held by ETFs?

If so, is that necessarily bad, or does it enable more efficient price discovery?

What are the effects on liquidity and capital formation?

Are the effects different depending on whether the growth is in passively managed ETFs, actively managed ETFs, ETMFs, or other ETPs?

Are there systemic risks that we should be monitoring?

ETFs, unlike mutual funds, rely on an interconnected web of participants, some of whom are affiliated with large banks.

What happens if one of the authorized participants drops out of the market?
Will others pick up the slack, even in times of stress?

If not, what are the consequences?

Would there be larger spreads in the secondary market?

If yes, how would investors react?

What happens if one or more ETFs suspend the creation and redemption process?

As ETFs increasingly invest in less liquid assets, could redemptions amplify fire sale risks?

The answers to these questions are less clear than the potential benefits to investors, which are significant.

Nevertheless, answering these questions is critical to protecting investors, ensuring fair, orderly and efficient markets, and facilitating capital formation —broad goals that include financial stability.

I worry that these larger questions have been getting lost in the current ETF exemptive application and exchange listing process, where each product is considered independently, without the kind of broad attention that is necessary to garner the depth of public input I think we need on these questions.

The Commission has a cross-divisional team that is monitoring the growing ETP industry and its broader market and systemic impacts.

This is an area where we would benefit immensely from public input.

I have therefore asked the Chair to have the staff prioritize a written request for comment to the Commission to provide a formal mechanism for getting public input on these and other issues related to ETPs.

Conclusion

I have covered a lot and want to leave you with three thoughts.

First, we have the most vibrant financial markets in the world because they are so transparent.
History has demonstrated time and time again that modest up-front costs that come from additional transparency are more than made up for by the added liquidity, reliability, and competitive returns that come when markets function as they should.

Second, transparency matters to both retail and institutional investors.

Last, as we consider changes in transparency, for example in areas like ETFs, we must be cognizant of the broader effects on our markets and the entire financial system.

Thank you for inviting me to be with you this afternoon.

I look forward to hearing your thoughts and working on these issues with you going forward.

Ten Ways to Improve the Security of a New Computer

Jennifer Kent and Katie Steiner

Why Should I Care About Computer Security?

Our computers help us stay connected to the modern world.

We use them for banking and bill paying, shopping, connecting with our friends and family through email and social networking sites, surfing the internet, and so much more.

We rely so heavily on our computers to provide these services that we sometimes overlook their security.

Because our computers have such critical roles in our lives and we trust them with so much personal information, it's important to improve their security so we can continue to rely on them and keep our information safe.

Attackers can infect your computer with malicious software, or malware, in many different ways.

They can take advantage of unsafe user practices and flaws in your computer's programs (flaws including vulnerabilities and unsecured services and features) and use social engineering (in which an attacker convinces someone to perform an action such as opening a malicious email attachment or following a malicious link).

Once your computer is infected, intruders can use the malware to access your computer without your knowledge to perform unwanted actions.

They can steal your personal information, change computer configurations, cause your computer to perform unreliably, and install even more malware they can use to leverage attacks or spread malware to others.

One of the most well-known attacks was the Conficker malware detected in late 2008.

This malware grew to become one of the largest malware infections, affecting millions of computers and causing billions of dollars in damage across the world.

The Conficker malware had the ability to steal and relay personal information to attackers, disable existing security measures like Windows Automatic Updates and antivirus software, and block internet access to popular security websites.

Attackers could use infected computers as part of a botnet, or a collection of compromised computers connected to the internet, to leverage additional attacks against other computers.

The Conficker malware took advantage of three separate security flaws on Microsoft Windows computers: the enabled file sharing service, the default AutoRun setting, and a vulnerability in the Windows Server network service. If people had used the following ten practices, the risk of infection of Conficker would have been significantly reduced.

How Do I Improve the Security of My Home Computer?

Following are ten important things you can do to make your home computer more secure.

While no individual step will completely eliminate your risk, together these practices will make your home computer's defense strong and minimize the threat of malicious activity.

1. Connect to a Secure Network

Once your computer is connected to the internet, it's also connected to millions of other connected computers, which could, in turn, allow attackers to connect to your computer.

Information flows from the internet to your home network by first coming into your modem, then to your router, which most people have, and finally to your computer.

Because your modem doesn't have security settings, it's crucial to secure your router—the first securable device that receives information from the internet.

Be sure to secure it before you connect to the internet to improve your computer's security.

If you don't have a router, contact your service provider to learn how you can best secure your network.

The default configurations of most home routers offer little security.

Though it may seem cumbersome to spend time configuring your router's settings, it's well worth it because a secure router is one of the best initial lines of defense.

To secure your router, consult its user's guide, which will direct you to a predefined URL or IP address where you can do the following:

- Configure the wireless network to use WPA2-AES encryption for data confidentiality.

- Change the default login username, if permitted (refer to the user's guide), and password. (The default passwords are published in manufacturer's publications and are readily accessible.)

- Conduct MAC address filtering (a form of whitelisting, or identifying wirelessly connected computers you trust).

- Change the default wireless SSID.

Learn more about each of these configurations and others in the document "Small Office/Home Office Router Security" (http://www.us-cert.gov/reading_room/HomeRouterSecurity2011.pdf).

2. Enable and Configure a Firewall

A firewall is a device that controls the flow of information between your computer and the internet, similar to a router.

Most modern operating systems include a software firewall.

In addition to the operating system's firewall, the majority of home routers have a firewall built in.

Refer to your user's guide for instructions on how to enable your firewall.

Once your firewall is enabled, consult the user's guide to learn how to configure the security settings and set a strong password to protect it against unwanted changes.

3. Install and Use Antivirus and Antispyware Software

Installing an antivirus and antispyware software program and keeping it up to date is a critical step in protecting your computer.

Many types of antivirus and antispyware software can detect the possible presence of malware by looking for patterns in the files or memory of your computer.

This software uses virus signatures provided by software vendors to look for malware.

New malware is discovered daily, and vendors frequently make new signatures available, so antivirus software will be most effective if the signatures are up to date.

Many antivirus and antispyware programs offer automatic updating.

Enable that feature so your software always has the most current signatures.

If automatic updates aren't offered, be sure to install the software from a reputable source, like the vendor's website or a CD from the vendor.

4. Remove Unnecessary Software

Intruders can attack your computer by exploiting software vulnerabilities (that is, flaws or weaknesses), so the less software you have installed, the fewer avenues for potential attack. Check the software installed on your computer.

If you don't know what a software program does and don't use it, research it to determine whether it's necessary.

Remove any software you feel isn't necessary after confirming the software is safe to be removed.

Back up important files and data before removing unnecessary software in case you accidentally remove software essential to the operating system. If possible, locate the installation media for the software in case you need to reinstall it.

5. Disable Nonessential Services

Like unnecessary software, nonessential services increase the opportunities for attack.

Two services to look for are file sharing and print sharing, which enable you to share files, such as photos and music, with other computer users and print to other computers on your network.

The Conficker malware used file sharing to infect computers and spread the infection to others.

Disabling file sharing would have eliminated one of the ways Conficker infected computers at the time of the Conficker malware infection.

If those services are enabled in your operating system, disable them if you only have one computer connected to your network or don't use them. Because services differ depending on your operating system and many of them are critical to your computer's operation, research any services you aren't sure about or don't use before disabling them.

6. Modify Unnecessary Default Features

Like removing unnecessary software and disabling nonessential services, modifying unnecessary default features eliminates opportunities for attack. Review the features that came enabled by default on your computer and disable or customize those you don't need or plan on using.

As with nonessential services, be sure to research these features before disabling or modifying them.

The AutoRun feature in Microsoft Windows systems was a default feature at the time of the Conficker malware and was one of the three ways computers became infected.

When the AutoRun feature is enabled on Windows computers, Windows detects when removable media, such as CDs and USB storage devices, are inserted into the computer and automatically executes the media's contents.

7. Operate Under the Principle of Least Privilege

In most instances of a malware infection, the malware can operate only under the rights of the logged-in user.

To minimize the impact the malware can have if it successfully infects a computer, consider using a standard or restricted user account for day-to-day activities and only logging in with the administrator account (which has full operating privileges on the system) when you need to install or remove software or change system settings from the computer.

8. Secure Your Web Browser

Web browsers installed on new computers usually don't have secure default settings.

Securing your browser is another critical step in improving your computer's security because an increasing number of attacks take advantage of web browsers. Before you start surfing the internet, secure your browser by doing the following:

- Disable mobile code (that is, Java, JavaScript, Flash, and ActiveX) on websites you're not familiar with or don't trust. While disabling these types of code on all sites will significantly reduce your risk of being attacked, the websites you visit may not function as they normally do.

- Disable options to always set cookies. A cookie is a file placed on your computer that stores website data.

Attackers may be able to log onto a site you've visited (like a banking site) by accessing the cookie with your login information.

To prevent that, configure the browser to ask for permission before setting a cookie, allow cookies for sessions only, and disable features that keep you logged in to a site or that retain information you've entered, such as text you type into forms and the search bar.

- If you're using Internet Explorer, set the security levels for trusted sites (websites you most often visit and trust) to the second highest level.

At the highest level, websites may not function properly.

Learn how to adjust these and other critical settings for the three most common browsers— Internet Explorer, Mozilla Firefox, and Apple Safari— in the document "Securing Your Web Browser" (http://www.us-cert.gov/reading_room/securing_browser/).

9. Apply Software Updates and Enable Future Automatic Updates

Most software vendors release updates to patch or fix vulnerabilities, flaws, and weaknesses (bugs) in their software.

Because intruders can exploit these bugs to attack your computer, keeping your software updated is important to help prevent infection.

The third way Conficker attacked computers was by exploiting a vulnerability in Windows systems.

Microsoft provided an update for this vulnerability.

If people would have applied the update in a timely manner, they would have eliminated the opportunity for Conficker to infect their computers through this software vulnerability and helped reduce the spread of further Conficker infections across the internet.

When you set up a new computer (and after you have completed the previous practices), go to your software vendors' websites and check for and install all available updates.

Enable automatic updates if your vendors offer it; that will ensure your software is always updated, and you won't have to remember to do it yourself.

Many operating systems and software have options for automatic updates.

As you're setting up your new computer, be sure to enable these options if offered.

Be cautious, however, because intruders can set up malicious websites that look nearly identical to legitimate sites.

Only download software updates directly from a vendor's website, from a reputable source, or through automatic updating.

10. Use Good Security Practices

You can do some simple things to improve your computer's security. Some of the most important are

- Use caution with email attachments and untrusted links. Malware is commonly spread by people clicking on an email attachment or a link that launches the malware.

Don't open attachments or click on links unless you're certain they're safe, even if they come from a person you know.

Some malware sends itself through an infected computer.

While the email may appear to come from someone you know, it really came from a compromised computer.

Be especially wary of attachments with sensational names, emails that contain misspellings, or emails that try to entice you into clicking on a link or attachment (for example, an email with a subject like that reads, "Hey, you won't believe this picture of you I saw on the internet!").

- Use caution when providing sensitive information.

Some email or web pages that appear to come from a legitimate source may actually be the work of an attacker.

An example is an email claiming to be sent from a system administrator requesting your password or other sensitive information or directing you to a website requesting that information.

While internet service providers may request that you change your password, they will never specify what you should change it to or ask you what it is.

- Create strong passwords.

Passwords that have eight or more characters, use a variety of uppercase and lowercase letters, and contain at least one symbol and number are best.

Don't use passwords that people can easily guess like your birthday or your child's name.

Password detection software can conduct dictionary attacks to try common words that may be used as passwords or conduct brute-force attacks where the login screen is pummeled with random attempts until it succeeds.

The longer and more complex a password is, the harder these tools have to work to crack it.

Also, when setting security verification questions, choose questions for which it is unlikely that an internet search would yield the correct answer.

Where Can I Learn More?

Implementing the practices in this paper will significantly improve your computer's security.

The more you can implement, the more secure your computer will be.

Even after implementing all ten of these practices, you still may not be protected from all of the risks you and your computer may encounter.

It's important to continue investigating and implementing new ways to secure your computer because new risks will arise and old risks evolve.

Learn more from these US-CERT resources:

- "Small Office/Home Office Router Security" (http://www.us-cert.gov/reading_room/HomeRouterSecurity2011.pdf)
- "Socializing Securely: Using Social Networking Services" (http://www.us- cert.gov/reading_room/safe_social_networking.pdf)
- "Securing Your Web Browser" (http://www.us-cert.gov/reading_room/securing_browser/)

Home Network Security

This document provides home users an overview of the security risks and countermeasures associated with Internet connectivity, especially in the context of "always-on" or broadband access services (such as cable modems and DSL).

However, much of the content is also relevant to traditional dial-up users (users who connect to the Internet using a modem).

I. Computer security

A. What is computer security?

Computer security is the process of preventing and detecting unauthorized use of your computer.

Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system.

Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

B. Why should I care about computer security?

We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs.

Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer (such as financial statements).

C. Who would want to break into my computer at home?

Intruders (also referred to as hackers, attackers, or crackers) may not care about your identity.

Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.

Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems.

Even if you have a computer connected to the Internet only to play the latest games or to send email to friends and family, your computer may be a target.

Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.

D. How easy is it to break into my computer?

Unfortunately, intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software.

The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.

When holes are discovered, computer vendors will usually develop patches to address the problem(s).

However, it is up to you, the user, to obtain and install the patches, or correctly configure the software to operate more securely.

Most of the incident reports of computer break-ins received at the CERT/CC could have been prevented if system administrators and users kept their computers up-to-date with patches and security fixes.

Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure.

Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.

II. Technology

This section provides a basic introduction to the technologies that underlie the Internet.

It was written with the novice end-user in mind and is not intended to be a comprehensive survey of all Internet-based technologies.
Subsections provide a short overview of each topic.

This section is a basic primer on the relevant technologies.

For those who desire a deeper understanding of the concepts covered here, we include links to additional information.

A. What does "broadband" mean?

"Broadband" is the general term used to refer to high-speed network connections.

In this context, Internet connections via cable modem and Digital Subscriber Line (DSL) are frequently referred to as broadband Internet connections.

"Bandwidth" is the term used to describe the relative speed of a network connection -- for example, most current dial-up modems can support a bandwidth of 56 kbps (thousand bits per second).

There is no set bandwidth threshold required for a connection to be referred to as "broadband," but it is typical for connections in excess of 1 Megabit per second (Mbps) to be so named.

B. What is cable modem access?

A cable modem allows a single computer (or network of computers) to connect to the Internet via the cable TV network.

The cable modem usually has an Ethernet LAN (Local Area Network) connection to the computer and is capable of speeds in excess of 5 Mbps.

Typical speeds tend to be lower than the maximum, however, since cable providers turn entire neighborhoods into LANs that share the same bandwidth.

Because of this "shared-medium" topology, cable modem users may experience somewhat slower network access during periods of peak

demand and may be more susceptible to risks such as packet sniffing and unprotected windows shares than users with other types of connectivity.

(See the "Computer security risks to home users" section of this document.)

C. What is DSL access?

Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, provides the user with dedicated bandwidth.

However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies.

Also, the "dedicated bandwidth" is only dedicated between your home and the DSL provider's central office -- the providers offer little or no guarantee of bandwidth all the way across the Internet.

DSL access is not as susceptible to packet sniffing as cable modem access, but many of the other security risks we'll cover apply to both DSL and cable modem access. (See the "Computer security risks to home users" section of this document.)

D. How are broadband services different from traditional dial-up services?

Traditional dial-up Internet services are sometimes referred to as "dial-on-demand" services.

That is, your computer only connects to the Internet when it has something to send, such as email or a request to load a web page.

Once there is no more data to be sent, or after a certain amount of idle time, the computer disconnects the call.

Also, in most cases each call connects to a pool of modems at the ISP, and since the modem IP addresses are dynamically assigned, your computer is usually assigned a different IP address on each call.

As a result, it is more difficult (not impossible, just difficult) for an attacker to take advantage of vulnerable network services to take control of your computer.

Broadband services are referred to as "always-on" services because there is no call setup when your computer has something to send.

The computer is always on the network, ready to send or receive data through its network interface card (NIC).

Since the connection is always up, your computer's IP address will change less frequently (if at all), thus making it more of a fixed target for attack.

What's more, many broadband service providers use well-known IP addresses for home users.

So while an attacker may not be able to single out your specific computer as belonging to you, they may at least be able to know that your service provider's broadband customers are within a certain address range, thereby making your computer a more likely target than it might have been otherwise.

The table below shows a brief comparison of traditional dial-up and broadband services.

	Dial-up	Broadband
Connection type	Dial on demand	Always on
IP address	Changes on each call	Static or infrequently changing
Relative connection speed	Low	High
Remote control potential	Computer must be dialed in to control remotely	Computer is always connected, so remote control can occur anytime
ISP-provided security	Little or none	Little or none

Table 1: Comparison of Dial-up and Broadband Services

E. How is broadband access different from the network I use at work?

Corporate and government networks are typically protected by many layers of security, ranging from network firewalls to encryption.

In addition, they usually have support staff who maintain the security and availability of these network connections.

Although your ISP is responsible for maintaining the services they provide to you, you probably won't have dedicated staff on hand to manage and operate your home network.

You are ultimately responsible for your own computers.

As a result, it is up to you to take reasonable precautions to secure your computers from accidental or intentional misuse.

F. What is a protocol?

A protocol is a well-defined specification that allows computers to communicate across a network.

In a way, protocols define the "grammar" that computers can use to "talk" to each other.

G. What is IP?

IP stands for "Internet Protocol." It can be thought of as the common language of computers on the Internet.

There are a number of detailed descriptions of IP given elsewhere, so we won't cover it in detail in this document.

However, it is important to know a few things about IP in order to understand how to secure your computer.

Here we'll cover IP addresses, static vs. dynamic addressing, NAT, and TCP and UDP Ports.

An overview of TCP/IP can be found in the TCP/IP Frequently Asked Questions (FAQ) at the following URLs:

http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/
http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part2/

H. What is an IP address?

IP addresses are analogous to telephone numbers -- when you want to call someone on the telephone, you must first know their telephone number.

Similarly, when a computer on the Internet needs to send data to another computer, it must first know its IP address.

IP addresses are typically shown as four numbers separated by decimal points, or "dots."

For example, 10.24.254.3 and 192.168.62.231 are IP addresses.

If you need to make a telephone call but you only know the person's name, you can look them up in the telephone directory (or call directory services) to get their telephone number.

On the Internet, that directory is called the Domain Name System, or DNS for short.

If you know the name of a server, say www.cert.org, and you type this into your web browser, your computer will then go ask its DNS server what the numeric IP address is that is associated with that name.

Every computer on the Internet has an IP address associated with it that uniquely identifies it.

However, that address may change over time, especially if the computer is

- dialing into an Internet Service Provider (ISP)

- connected behind a network firewall

- connected to a broadband service using dynamic IP addressing

I. What are static and dynamic addressing?

Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user.

These addresses do not change over time. However, if a static address is assigned but not in use, it is effectively wasted.

Since ISPs have a limited number of addresses allocated to them, they sometimes need to make more efficient use of their addresses.

Dynamic IP addressing allows the ISP to efficiently utilize their address space.

Using dynamic IP addressing, the IP addresses of individual user computers may change over time.

If a dynamic address is not in use, it can be automatically reassigned to another computer as needed.

J. What is NAT?

Network Address Translation (NAT) provides a way to hide the IP addresses of a private network from the Internet while still allowing computers on that network to access the Internet.

NAT can be used in many different ways, but one method frequently used by home users is called "masquerading."

Using NAT masquerading, one or more devices on a LAN can be made to appear as a single IP address to the outside Internet.

This allows for multiple computers in a home network to use a single cable modem or DSL connection without requiring the ISP to provide more than one IP address to the user.

Using this method, the ISP-assigned IP address can be either static or dynamic.

Most network firewalls support NAT masquerading.

K. What are TCP and UDP ports?

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both protocols that use IP.

Whereas IP allows two computers to talk to each other across the Internet, TCP and UDP allow individual applications (also known as "services") on those computers to talk to each other.

In the same way that a telephone number or physical mail box might be associated with more than one person, a computer might have multiple applications (e.g., email, file services, web services) running on the same IP address.

Ports allow a computer to differentiate services such as email data from web data.

A port is simply a number associated with each application that uniquely identifies that service on that computer.
Both TCP and UDP use ports to identify services. Some common port numbers are 80 for web (HTTP), 25 for email (SMTP), and 53 for Domain Name System (DNS).

L. What is a firewall?

The Firewalls FAQ (http://www.faqs.org/faqs/firewalls-faq/) defines a firewall as "a system or group of systems that enforces an access control policy between two networks."

In the context of home networks, a firewall typically takes one of two forms:

Software firewall - specialized software running on an individual computer, or

Network firewall - a dedicated device designed to protect one or more computers.

Both types of firewall allow the user to define access policies for inbound connections to the computers they are protecting.

Many also provide the ability to control what services (ports) the protected computers are able to access on the Internet (outbound access).

Most firewalls intended for home use come with pre-configured security policies from which the user chooses, and some allow the user to customize these policies for their specific needs.

More information on firewalls can be found in the Additional resources section of this document.

M. What does antivirus software do?

There are a variety of antivirus software packages that operate in many different ways, depending on how the vendor chose to implement their software.

What they have in common, though, is that they all look for patterns in the files or memory of your computer that indicate the possible presence of a known virus.

Antivirus packages know what to look for through the use of virus profiles (sometimes called "signatures") provided by the vendor.

New viruses are discovered daily. The effectiveness of antivirus software is dependent on having the latest virus profiles installed on your computer so

that it can look for recently discovered viruses. It is important to keep these profiles up to date.

III. Computer security risks to home users

A. What is at risk?

Information security is concerned with three main areas:

Confidentiality -- information should be available only to those who rightfully have access to it

Integrity -- information should be modified only by those who are authorized to do so

Availability -- information should be accessible to those who need it when they need it

These concepts apply to home Internet users just as much as they would to any corporate or government network.

You probably wouldn't let a stranger look through your important documents.

In the same way, you may want to keep the tasks you perform on your computer confidential, whether it's tracking your investments or sending email messages to family and friends.

Also, you should have some assurance that the information you enter into your computer remains intact and is available when you need it.

Some security risks arise from the possibility of intentional misuse of your computer by intruders via the Internet.

Others are risks that you would face even if you weren't connected to the Internet (e.g. hard disk failures, theft, power outages).

The bad news is that you probably cannot plan for every possible risk.

The good news is that you can take some simple steps to reduce the chance that you'll be affected by the most common threats -- and some of those steps help with both the intentional and accidental risks you're likely to face.

Before we get to what you can do to protect your computer or home network, let's take a closer look at some of these risks.

B. Intentional misuse of your computer

The most common methods used by intruders to gain control of home computers are briefly described below.

More detailed information is available by reviewing the URLs listed in the References section below.

Trojan horse programs
Back door and remote administration programs
Denial of service
Being an intermediary for another attack
Unprotected Windows shares
Mobile code (Java, JavaScript, and ActiveX)
Cross-site scripting
Email spoofing
Email-borne viruses
Hidden file extensions
Chat clients
Packet sniffing

Trojan horse programs

Trojan horse programs are a common way for intruders to trick you (sometimes referred to as "social engineering") into installing "back door" programs.

These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus.

More information about Trojan horses can be found in the following document:
http://www.cert.org/advisories/CA-1999-02.html

Back door and remote administration programs

On Windows computers, three tools commonly used by intruders to gain remote access to your computer are BackOrifice, Netbus, and SubSeven.

These back door or remote administration programs, once installed, allow other people to access and control your computer.

Denial of service

Another form of attack is called a denial-of-service (DoS) attack.

This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. In most cases, the latest patches will prevent the attack.

The following documents describe denial-of-service attacks in greater detail.

http://www.cert.org/advisories/CA-2000-01.html

http://www.cert.org/archive/pdf/DoS_trends.pdf

It is important to note that in addition to being the target of a denial-of-service attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

Being an intermediary for another attack

Intruders will frequently use compromised computers as launching pads for attacking other systems.

An example of this is how distributed denial-of-service (DDoS) tools are used.

The intruders install an "agent" (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions.

Then, when a number of agents are running on different computers, a single "handler" can instruct all of them to launch a denial-of-service attack on another system.

Thus, the end target of the attack is not your own computer, but someone else's -- your computer is just a convenient tool in a larger attack.

Unprotected Windows shares

Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet.

Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet.

The greater immediate risk to the Internet community is the potentially large number of computers attached to the Internet with unprotected Windows networking shares combined with distributed attack tools such as those described in
http://www.cert.org/incident_notes/IN-2000-01.html

Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate. One such example is the 911 worm described in
http://www.cert.org/incident_notes/IN-2000-03.html

There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

Mobile code (Java, JavaScript, and ActiveX)

There have been reports of problems with "mobile code" (e.g., Java, JavaScript, and ActiveX).

These are programming languages that let web developers write code that is executed by your web browser.

Although the code is generally useful, it can be used by intruders to gather information (such as which websites you visit) or to run malicious code on your computer.

It is possible to disable Java, JavaScript, and ActiveX in your web browser.

We recommend that you do so if you are browsing websites that you are not familiar with or do not trust.

Also be aware of the risks involved in the use of mobile code within email programs. Many email programs use the same code as web browsers to

display HTML. Thus, vulnerabilities that affect Java, JavaScript, and ActiveX are often applicable to email as well as web pages.

More information on ActiveX security is available in http://www.cert.org/archive/pdf/activeX_report.pdf.

Cross-site scripting

A malicious web developer may attach a script to something sent to a website, such as a URL, an element in a form, or a database inquiry.

Later, when the website responds to you, the malicious script is transferred to your browser.

You can potentially expose your web browser to malicious scripts by following links in web pages, email messages, or newsgroup postings without knowing what they link to using interactive forms on an untrustworthy site viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags

More information regarding the risks posed by malicious code in web links can be found in CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests.

Email spoofing

Email "spoofing" is when an email message appears to have originated from one source when it actually was sent from another source.

Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Spoofed email can range from harmless pranks to social engineering ploys.

Examples of the latter include

- email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not comply

- email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information
Note that while service providers may occasionally request that you change your password, they usually will not specify what you should change it to.

Also, most legitimate service providers would never ask you to send them any password information via email.

If you suspect that you may have received a spoofed email from someone with malicious intent, you should contact your service provider's support personnel immediately.

Email-borne viruses

Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know the source of the attachment.

It is not enough that the mail originated from an address you recognize. The Melissa virus (see References) spread precisely because it originated from a familiar address.

Also, malicious code might be distributed in amusing or enticing programs.

Many recent viruses use these social engineering techniques to spread.

Examples include
W32/Sircam -- http://www.cert.org/advisories/CA-2001-22.html
W32/Goner -- http://www.cert.org/incident_notes/IN-2001-15.html

Never run a program unless you know it to be authored by a person or company that you trust.

Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program.

Hidden file extensions

Windows operating systems contain an option to "Hide file extensions for known file types."

The option is enabled by default, but a user may choose to disable this option in order to have file extensions displayed by Windows.
Multiple email-borne viruses are known to exploit hidden file extensions. The first major attack that took advantage of a hidden file extension was the VBS/LoveLetter worm which contained an email attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs".

Other malicious programs have since incorporated similar naming schemes.

Examples include
Downloader (MySis.avi.exe or QuickFlick.mpg.exe)
VBS/Timofonica (TIMOFONICA.TXT.vbs)
VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs)
VBS/OnTheFly (AnnaKournikova.jpg.vbs)

The files attached to the email messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or executable (.vbs or .exe, for example).

Chat clients

Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet.

Chat clients provide groups of individuals with the means to exchange dialog, web URLs, and in many cases, files of any type.

Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients.

As with email clients, care should be taken to limit the chat client's ability to execute downloaded files. As always, you should be wary of exchanging files with unknown parties.

Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network.

That data may include user names, passwords, and proprietary information that travels over the network in clear text.

With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems.

Installing a packet sniffer does not necessarily require administrator-level access.

Relative to DSL and traditional dial-up users, cable modem users have a higher risk of exposure to packet sniffers since entire neighborhoods of cable modem users are effectively part of the same LAN.

A packet sniffer installed on any cable modem user's computer in a neighborhood may be able to capture data transmitted by any other cable modem in the same neighborhood.

C. Accidents and other risks

In addition to the risks associated with connecting your computer to the Internet, there are a number of risks that apply even if the computer has no network connections at all.

Most of these risks are well known, so we won't go into much detail in this document, but it is important to note that the common practices associated with reducing these risks may also help reduce susceptibility to the network-based risks discussed above.

Disk failure

Recall that availability is one of the three key elements of information security.

Although all stored data can become unavailable -- if the media it's stored on is physically damaged, destroyed, or lost -- data stored on hard disks is at higher risk due to the mechanical nature of the device.

Hard disk crashes are a common cause of data loss on personal computers.

Regular system backups are the only effective remedy.

Power failure and surges

Power problems (surges, blackouts, and brown-outs) can cause physical damage to a computer, inducing a hard disk crash or otherwise harming the electronic components of the computer.
Common mitigation methods include using surge suppressors and uninterruptible power supplies (UPS).

Physical theft

Physical theft of a computer, of course, results in the loss of confidentiality and availability, and (assuming the computer is ever recovered) makes the integrity of the data stored on the disk suspect.

Regular system backups (with the backups stored somewhere away from the computer) allow for recovery of the data, but backups alone cannot address confidentiality.

Cryptographic tools are available that can encrypt data stored on a computer's hard disk.

The CERT/CC encourages the use of these tools if the computer contains sensitive data or is at high risk of theft (e.g., laptops or other portable computers).

IV. Actions home users can take to protect their computer systems

The CERT/CC recommends the following practices to home users:

Consult your system support personnel if you work from home
Use virus protection software
Use a firewall
Don't open unknown email attachments
Don't run programs of unknown origin
Disable hidden filename extensions
Keep all applications, including your operating system, patched
Turn off your computer or disconnect from the network when not in use
Disable Java, JavaScript, and ActiveX if possible
Disable scripting features in email programs
Make regular backups of critical data
Make a boot disk in case your computer is damaged or compromised

Further discussion on each of these points is given below.

Recommendations

Consult your system support personnel if you work from home

If you use your broadband access to connect to your employer's network via a Virtual Private Network (VPN) or other means, your employer may have policies or procedures relating to the security of your home network.

Be sure to consult with your employer's support personnel, as appropriate, before following any of the steps outlined in this document.

Use virus protection software

The CERT/CC recommends the use of antivirus software on all Internet-connected computers.

Be sure to keep your antivirus software up to date.

Many antivirus packages support automatic updates of virus definitions.

We recommend the use of these automatic updates when available.

Use a firewall

We strongly recommend the use of some type of firewall product, such as a network appliance or a personal firewall software package.

Intruders are constantly scanning home user systems for known vulnerabilities.

Network firewalls (whether software or hardware-based) can provide some degree of protection against these attacks.

However, no firewall can detect or stop all attacks, so it's not sufficient to install a firewall and then ignore all other security measures.

Don't open unknown email attachments

Before opening any email attachments, be sure you know the source of the attachment.

It is not enough that the mail originated from an address you recognize.

The Melissa virus spread precisely because it originated from a familiar address.

Malicious code might be distributed in amusing or enticing programs.

If you must open an attachment before you can verify the source, we suggest the following procedure:

- Be sure your virus definitions are up to date (see "Use virus protection software" above).

- Save the file to your hard disk.

- Scan the file using your antivirus software.

- Open the file.

For additional protection, you can disconnect your computer's network connection before opening the file.

Following these steps will reduce, but not wholly eliminate, the chance that any malicious code contained in the attachment might spread from your computer to others.

Don't run programs of unknown origin

Never run a program unless you know it to be authored by a person or company that you trust.

Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing--they might contain a Trojan horse program.

Disable hidden filename extensions

Windows operating systems contain an option to "Hide file extensions for known file types."

The option is enabled by default, but you can disable this option in order to have file extensions displayed by Windows.

After disabling this option, there are still some file extensions that, by default, will continue to remain hidden.

There is a registry value which, if set, will cause Windows to hide certain file extensions regardless of user configuration choices elsewhere in the operating system.

The "NeverShowExt" registry value is used to hide the extensions for basic Windows file types.

For example, the ".LNK" extension associated with Windows shortcuts remains hidden even after a user has turned off the option to hide extensions.

Specific instructions for disabling hidden file name extensions are given in http://www.cert.org/incident_notes/IN-2000-07.html.

Keep all applications, including your operating system, patched

Vendors will usually release patches for their software when a vulnerability has been discovered.

Most product documentation offers a method to get updates and patches.

You should be able to obtain updates from the vendor's website.

Read the manuals or browse the vendor's website for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list.

Look on your vendor's website for information about automatic notification.

If no mailing list or other automated notification mechanism is offered, you may need to check periodically for updates.

Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it.

An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

Disable Java, JavaScript, and ActiveX if possible

Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript.

A malicious web developer may attach a script to something sent to a website, such as a URL, an element in a form, or a database inquiry.

Later, when the website responds to you, the malicious script is transferred to your browser.

The most significant impact of this vulnerability can be avoided by disabling all scripting languages.

Turning off these options will keep you from being vulnerable to malicious scripts.

However, it will limit the interaction you can have with some websites.

Many legitimate sites use scripts running within the browser to add useful features. Disabling scripting may degrade the functionality of these sites.

More information on ActiveX security, including recommendations for users who administer their own computers, is available in http://www.cert.org/archive/pdf/activeX_report.pdf.

More information regarding the risks posed by malicious code in web links can be found in CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests.

Disable scripting features in email programs

Because many email programs use the same code as web browsers to display HTML, vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to email as well as web pages.

Therefore, in addition to disabling scripting features in web browsers (see "Disable Java, JavaScript, and ActiveX if possible" above), we recommend that users also disable these features in their email programs.

Make regular backups of critical data

Keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks).

Use software backup tools if available, and store the backup disks somewhere away from the computer.

Make a boot disk in case your computer is damaged or compromised

To aid in recovering from a security breach or hard disk failure, create a boot disk on a floppy disk, which will help when recovering a computer after such an event has occurred.

Remember, however, you must create this disk before you have a security event.

Virus Basics

US-CERT offers many resources to help you create a more secure home computing environment.

What is a virus?

A computer virus is a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files.

Viruses used to be spread when people shared floppy disks and other portable media, now viruses are primarily spread through email messages.

Unlike worms, viruses often require some sort of user action (e.g., opening an email attachment or visiting a malicious web page) to spread.

What do viruses do?

A virus is simply a computer program--it can do anything that any other program you run on your computer can do.

Some viruses are designed to deliberately damage files, and others may just spread to other computers.

What is a worm?

A worm is a type of virus that can spread without human interaction.

Worms often spread from computer to computer and take up valuable memory and network bandwidth, which can cause a computer to stop responding.

Worms can also allow attackers to gain access to your computer remotely.

What is a Trojan horse?

A Trojan horse is a computer program that is hiding a virus or other potentially damaging program.

A Trojan horse can be a program that purports to do one action when, in fact, it is performing a malicious action on your computer.

Trojan horses can be included in software that you download for free or as attachments in email messages.

Can I get a virus by reading my email messages?

Most viruses, Trojan horses, and worms are activated when you open an attachment or click a link contained in an email message.

If your email client allows scripting, then it is possible to get a virus by simply opening a message.

It's best to limit what HTML is available in your email messages. The safest way to view email messages is in plain text.

How can I avoid a virus infection from email?

Most users get viruses from opening and running unknown email attachments. Never open anything that is attached to an email message unless you know the contents of the file.

If you receive an attachment from a familiar email address, but were not expecting anything, you should contact the sender before opening the attachment.

If you receive a message with an attachment and you do not recognize the sender, you should delete the message.

Selecting the option to view your email messages in plain text, not HTML, will also help you to avoid a virus.

What are some tips to avoid viruses and lessen their impact?

- Install anti-virus software from a reputable vendor. Update it and use it regularly.

- In addition to scanning for viruses on a regular basis, install an "on access" scanner (included in most anti-virus software packages) and configure it to start each time you start up your computer. This will protect your system by checking for viruses each time you run an executable file.

- Use a virus scan before you open any new programs or files that may contain executable code. This includes packaged software that you buy from the store as well as any program you might download from the Internet.

- If you are a member of an online community or chat room, be very careful about accepting files or clicking links that you find or that people send you within the community.

- Make sure you back up your data (documents, bookmark files, important email messages, etc.) on disc so that in the event of a virus infection, you do not lose valuable work.

Understanding better the National Cybersecurity and Communications Integration Center

The Department of Homeland Security is responsible for protecting critical infrastructure from physical and cyber threats.

Cyberspace enables businesses and government to operate, facilitates emergency preparedness communications, and enables critical control systems processes.

Protecting these systems is essential to the resilience and reliability of the critical infrastructure and key resources and to the economic and national security.

NCCIC Overview

The NCCIC serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts.

NCCIC's partners include other government agencies, the private sector, and international entities.

Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts.

NCCIC Vision

To operate at the intersection of government, private sector, and international network defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response, mitigation, and recovery efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains.

NCCIC Mission

To operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique

analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the Constitutional and privacy rights of Americans in both the Cybersecurity and communications domains.

The NCCIC's missions include:

- Leading the protection of federal civilian agencies in cyberspace;

- Working closely together with critical infrastructure owners and operators to reduce risk;

- Collaborating with state and local governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC);

- Cooperating with international partners to share information and respond to incidents;

- Coordinating national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan (NCIRP);

- Analyzing data to develop and share actionable mitigation recommendations

- Creating and maintaining shared situational awareness among its partners and constituents;

- Orchestrating national protection, prevention, mitigation, and recovery activities associated with significant cyber and communication incidents;

- Disseminating cyber threat and vulnerability analysis information;

- Assisting in the initiation, coordination, restoration, and reconstitution of National Security or Emergency Preparedness (NS/EP) telecommunications services and facilities under all conditions, crises, or emergencies; and

- Executing Emergency Support Function 2- Communications (ESF-2) responsibilities under the National Response Framework (NRF).

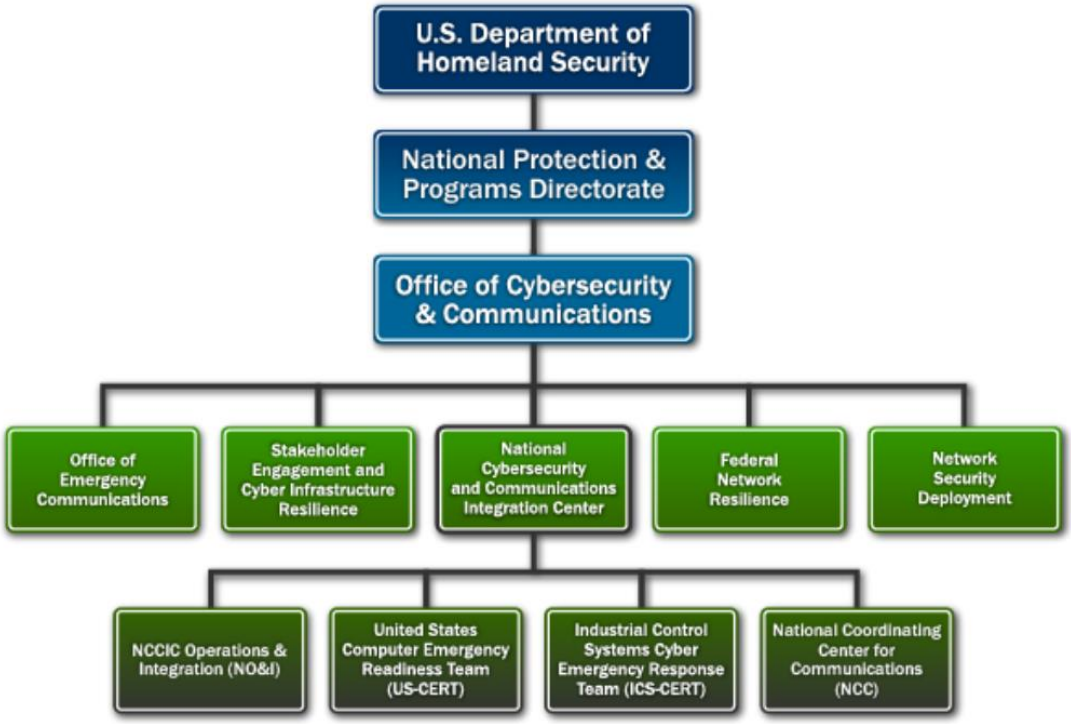
The NCCIC is comprised of four branches:

- NCCIC Operations & Integration (NO&I);

- United States Computer Emergency Readiness Team (US-CERT);

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and

- National Coordinating Center for Communications (NCC).



As mutually supporting, fully integrated elements of the NCCIC, these branches provide the authorities, capabilities, and partnerships necessary to lead a whole-of-nation approach to addressing cybersecurity and communications issues at the operational level.

NO&I plans, coordinates, and integrates capabilities to synchronize analysis, information sharing, and incident management efforts across the NCCIC's branches and activities.

US-CERT brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks.

US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners.

In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.

ICS-CERT reduces risk to the nation's critical infrastructure by strengthening control systems security through public-private partnerships.

ICS-CERT has four focus areas: situational awareness for CIKR stakeholders; control systems incident response and technical analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies.

NCC leads and coordinates the initiation, restoration, and reconstitution of NS/EP telecommunications services or facilities under all conditions.

NCC leverages partnerships with government, industry and international partners to obtain situational awareness and determine priorities for protection and response.

The NCCIC relies heavily on voluntary collaboration with its partners.

The NCCIC works closely with federal departments and agencies and actively engages with private sector companies and institutions, along with state, local, tribal, and territorial governments, and international counterparts.

Each group of stakeholders represents a community of practice, working together to protect the portions of critical information technology that they own, operate, manage, or interact with.

Give Yourself the Gift of Online Security

According to the National Retail Federation, 141 million people spent $57.4 billion dollars during Thanksgiving weekend last year, and consumers spent nearly $600 billion during the 2013 holiday season.

The biggest shopping season of the year comes with great deals and benefits to shoppers, but it also comes with certain risks.

While 80 percent of annual online sales occur between Black Friday and the weekend before Christmas, those four weeks are also the biggest weeks for online spammers and scammers.

With the holiday season quickly approaching, the best gift you can give yourself and your family is the gift of online security.

The following tips can help you protect your personal information when shopping online:

- Use and maintain anti-virus software and a firewall. Protect yourself against viruses and Trojan horses that may steal or modify the data on your computer and leave you vulnerable.

- Evaluate your software's settings. The default settings for most software enable all available functionality, possibly leaving room for an attacker to access your computer remotely.

Check the settings for all software, and especially those programs that connect to the Internet (browsers, email clients, mobile applications, etc.).

Apply the highest level of security available that still gives you the functionality you need.

- Shop on reliable websites. Take a look at the website's trademark or logo to make sure it's valid.

Also, pay attention to the website's URL.

Malicious websites may look identical to a legitimate website, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

- Protect your personal information. Take the time to check a website's privacy policy and understand what personal information is being requested and how it will be used.

If there is no policy cited, this could be a red flag that your personal information may be sold without your permission.

- Beware of deals that sound too good to be true. Use caution when opening email attachments and don't follow web links included in unsolicited email messages.

Watch out for extremely low prices on hard-to-get holiday items. If an offer seems too good to be true, it probably is.

- Look for the lock. When shopping online, check the lower-right corner of your screen for the padlock symbol and make sure the website address begins with "https://" before entering your shipping, billing, or payment information.

This symbol means that you're using a website that is secure and which encrypts the data you send or receive.

- Keep a record of your order. Retain all documentation of your online orders in the event that your purchase does not ship or there are unauthorized charges on your credit or debit card.

Also, be sure to review your credit card statement each month for irregularities.

- Get savvy about Wi - Fi hotspots. Limit the type of business you conduct when using public Wi-Fi networks.

Avoid shopping online when using public Wi-Fi as your information can easily be accessed by hackers on a public network.

If you think you have become a victim of identity theft, file a report with the Internet Crime Complaint Center.

You can also report online fraud to the Federal Trade Commission and file a report with the Department of Justice.

The Department of Homeland Security's Stop.Think.Connect.™ campaign encourages everyone to be vigilant about daily Internet use.

The campaign's objective is to increase the public's understanding of cyber threats and empower them to be safer and more secure online.
For more information, please visit www.dhs.gov/stopthinkconnect.

NIST Special Publication 800-171
Initial Public Draft

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology

RON ROSS, PATRICK VISCUSO, GARY GUISSANIE, KELLEY DEMPSEY
MARK RIDDLE

The protection of sensitive unclassified federal information while residing in nonfederal information systems and environments of operation is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.

This publication provides federal agencies with recommended requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) as defined by Executive Order 13556, when such information resides in nonfederal information systems and organizations. The requirements apply to:

(i) nonfederal information systems that are beyond the scope of the systems covered by the Federal Information Security Management Act (FISMA); and

(ii) all components of nonfederal systems that process, store, or transmit CUI

Notes to Reviewers

Executive Order 13556, Controlled Unclassified Information, November 4, 2010, establishes that the Controlled Unclassified Information (CUI) Executive Agent designated as the National Archives and Records Administration (NARA), "shall develop and issue such directives as are necessary" to implement the CUI Program.

Consistent with this tasking, and with the CUI Program's mission to establish uniform policies and practices across the federal government, NARA is issuing a Federal regulation, or directive, to establish the required controls and markings governmentwide.

A regulation binds agencies throughout the Executive branch to uniformly apply the Program's standard safeguards, markings, dissemination, and decontrol requirements.

The proposed rule, currently under Office of Management and Budget (OMB) coordination, contains a system of requirements that NARA developed in consultation with affected stakeholders, including nonfederal partners.

With regard to information systems, requirements for protection of CUI at the moderate confidentiality impact level in the proposed rule are based on applicable governmentwide standards and guidelines issued by NIST, and applicable policies established by OMB.

The proposed rule does not create these standards, which are already established by OMB and NIST.

Rather, the proposed rule requires the use of these standards in the same way throughout the Executive branch, thereby reducing current complexity for federal agencies and their nonfederal information-sharing partners, including contractors.

NARA has taken steps to alleviate the potential impact of the information security requirements on nonfederal organizations by jointly developing NIST Special Publication 800-171—thus, applying information security requirements, but based in the nonfederal environment.

Doing so should make it easier for nonfederal organizations to comply with the standards using the systems they already have in place, rather than trying to use government-specific approaches.

The CUI Executive Agent also anticipates establishing a single Federal Acquisition Regulation (FAR) clause that will apply the requirements of the proposed rule and NIST Special Publication 800-171 to the contractor environment.

This will further promote standardization to benefit a substantial number of nonfederal organizations that may struggle to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from different federal agencies for the same information gives rise to confusion and inefficiencies.

Until the formal process of establishing such a single FAR clause takes place, where necessitated by exigent circumstances, NIST Special Publication 800-171 may be referenced in a contract- specific requirement on a limited basis consistent with the regulatory requirements.

To summarize, in the process of this three-part plan (i.e., development of the CUI rule, NIST Special Publication, and standard FAR clause), nonfederal organizations, including contractors, will not only receive streamlined and uniform requirements for all CUI security needs, but also will have information security requirements for CUI tailored to nonfederal systems, allowing the nonfederal organizations to be in compliance with statutory and regulatory requirements, and to consistently implement safeguards for the protection of CUI.

Your feedback to us, as always, is important. We appreciate each and every contribution from our reviewers.

The very insightful comments from both the public and private sectors, nationally and internationally, continue to help shape our publications and ensure that they are meeting the needs and expectations of our customers.

Establishing Expectations for this Publication

This publication recognizes that—

- The security requirements contained herein, only apply to nonfederal information systems (or components of nonfederal systems) and organizations that process, store, or transmit Controlled Unclassified Information (CUI) as defined by Executive Order 13556.

- Nonfederal organizations are not developing or acquiring new information systems specifically for the purpose of processing, storing, or transmitting CUI—rather, these organizations already have an information technology infrastructure, acquisition process, and associated security policies, procedures, and practices in place.

Thus, federal information security requirements from FIPS Publication 200 and associated security controls from NIST Special Publication 800-53 in the Contingency Planning (CP) family, Planning (PL) family, System and Services Acquisition (SA) family, and Physical and Environmental Protection (PE) family (only requirements related to the environment in which the nonfederal system operates) have been deemed out of scope for this publication.

Policy- and procedure-related requirements and controls from the above publications have also been eliminated from consideration.

There are some exceptions where protecting CUI from disclosure may require some additional policies, procedures, and/or technologies that are beyond the standard practices one would anticipate finding in such organizations.

- Nonfederal organizations and their information systems may handle more than just federal information (e.g., CUI) and that there could be other constraints levied on those systems.

- There are many potential security solutions that can be implemented by nonfederal organizations to satisfy the security requirements—that is, alternative, but arguably equivalent methods may be employed.

- Nonfederal organizations may not always have the necessary organizational structure, resources, or infrastructure to satisfy every security requirement.

For example, very small businesses or contractors may have difficulty in satisfying the separation of duty requirement.

Federal agencies may consider such factors in their risk-based decisions and nonfederal organizations may in those situations, propose alternative security requirements that can compensate for the inability to satisfy a particular requirement.

INTRODUCTION - THE NEED TO PROTECT CONTROLLED UNCLASSIFIED INFORMATION

Today, more than at any time in history, the federal government is relying on external information system service providers to help carry out a wide range of federal missions and business functions.

Federal contractors, for example, routinely process, store, and transmit sensitive, unclassified federal information in their information systems to support the delivery of essential products and services to their federal customers (e.g., conducting basic or applied scientific research; conducting background investigations for security clearances; providing credit card and other financial services; providing Web support and electronic mail services; and developing healthcare, communications, and weapons systems).

The protection of sensitive, unclassified federal information while residing in nonfederal information systems and environments of operation is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions/business operations.

The protection of sensitive, unclassified federal information in nonfederal information systems and organizations is dependent on the federal government providing a disciplined and structured process for identifying the many different information/data types that are routinely used by federal agencies.

On November 4, 2010, the President signed Executive Order 13556, Controlled Unclassified Information (the Order).

The Order designated the National Archives and Records Administration (NARA) as the Executive Agent for Controlled Unclassified Information (CUI) and directed NARA to implement a governmentwide CUI Program to standardize the way the Executive branch handles unclassified information that requires protection.

Only information that requires safeguarding or dissemination controls pursuant to law, federal regulations, and governmentwide policies may be designated as CUI.

The CUI program is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry.

The CUI Registry:

(i) identifies the exclusive categories and subcategories of unclassified information that require safeguarding and dissemination controls consistent with law, federal regulation, and governmentwide policies; and

(ii) serves as the central repository for the posting of and access to the categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

The CUI Registry also includes the appropriate citation(s) of law, regulation, and/or governmentwide policy that form the basis for each category and subcategory.

The Order also required that the CUI Program emphasize openness, transparency, and uniformity of governmentwide practices and that the implementation of the program take place in a manner consistent with applicable policies established by the Office of Management and Budget (OMB) and federal standards and guidelines issued by the National Institute of Standards and Technology (NIST).

The federal CUI rule, developed by the CUI Executive Agent, provides guidance to federal agencies on the designation, safeguarding, dissemination, marking, decontrolling, and disposition of CUI, self-inspection and oversight requirements, and other facets of the program.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide federal agencies with recommended requirements for protecting the confidentiality of CUI when such information resides in nonfederal information systems and organizations.

The security requirements apply only to components of nonfederal information systems that process, store, or transmit CUI.

In accordance with the CUI rule issued by NARA, federal information systems that process, store, or transmit CUI, as a minimum, must comply with:

- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems (moderate impact value for confidentiality);

- Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems;

- NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (moderate baseline as tailored by the implementing organization); and

- NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

The requirements for protecting the confidentiality of CUI in nonfederal information systems have been derived from the above authoritative publications using the design criteria described in Chapter 2.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience including:

- Individuals with information system development life cycle responsibilities (e.g., program managers, information owners/stewards, mission/business owners, information system owners, acquisition/procurement officials);

- Individuals with information system, security, and/or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, information system managers, information security managers); and

- Individuals with information security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts).

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- Chapter Two describes the assumptions and methodology used in developing the security requirements to protect the confidentiality of CUI in nonfederal information systems and organizations and options that can be employed by nonfederal organizations to determine compliance to such requirements.

- Chapter Three describes the fourteen families of security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations.

- Supporting appendices provide additional information related to the protection of CUI in nonfederal information systems and organizations including:

(i) general references;

(ii) definitions and terms; and

(iii) acronyms.

CHAPTER TWO

THE FUNDAMENTALS
ASSUMPTIONS AND METHODOLOGY FOR DEVELOPING CUI SECURITY REQUIREMENTS

This chapter:

(i) describes the assumptions and methodology used in developing the security requirements to protect CUI in nonfederal information systems and organizations; and

(ii) discusses the potential assessment options that can be employed to determine compliance to the CUI security requirements.

2.1 CONSTRUCTION OF CUI SECURITY REQUIREMENTS

The security requirements described in this publication have been developed based on three fundamental assumptions:

- Statutory and regulatory requirements for the protection of CUI are consistent, whether such information resides in federal information systems or nonfederal information systems including the environments in which those systems operate;

- Safeguards or countermeasures implemented to protect CUI are consistent in both federal and nonfederal environments; and

- The confidentiality impact value for CUI is no lower than moderate in accordance with Federal Information Processing Standards (FIPS) Publication 199.

The above assumptions reinforce the concept that federal information designated as CUI has the same intrinsic value and potential adverse impact if compromised—whether such information resides in a federal agency or a nonfederal organization.

Thus, protecting the confidentiality of CUI is critical to the mission and business success of federal agencies.

Security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have a well-defined structure that consists of the following:

(i) a basic security requirement section;

(ii) a derived security requirements section; and

(iii) a reference section.

The basic security requirements are obtained from FIPS Publication 200 and tailored appropriately to eliminate requirements that are:

- Primarily the responsibility of the federal government (i.e., uniquely federal);

- Related primarily to availability; or

- Assumed to be routinely satisfied by nonfederal organizations without any further specification.

The derived security requirements, which supplement the basic security requirements, are taken from the security control language in NIST Special Publication 800-53.

Starting with the moderate security control baseline (i.e., the minimum level of protection for CUI in federal information systems), the SP 800-53 controls are tailored using the same criteria used to tailor the FIPS 200 requirements.

After tailoring the moderate baseline to eliminate security controls that are uniquely federal, availability-related, and assumed to be routinely satisfied by nonfederal organizations without further specification, the remaining control language (not already included in the basic security requirement) forms the basis of the derived security requirements.
The combination of the basic and derived security requirements captures the intent of FIPS 200 and SP 800-53, with respect to the protection of the confidentiality of CUI in nonfederal information systems and organizations.

Finally, the references section includes a listing of the security controls from SP 800-53 that provides the basis, along with FIPS 200, for the security requirements.

The security control references are included to provide additional reference material to nonfederal organizations to promote a better understanding of the requirements.

To read more: http://csrc.nist.gov/publications/drafts/800-171/sp800_171_draft.pdf

Statement on Proposed 2015 Budget and Strategic Plan

Jeanette M. Franzel, Board Member
PCAOB Open Board Meeting
Washington, DC

I support the proposed 2015 budget and the 2014-2018 strategic plan being presented to the Board today.

I commend the staff for its rigorous review of programs and activities in developing a more conservative approach to estimating the budget for PCAOB.

This more conservative approach to our budget improves our ability to be careful stewards of the funds we rely upon, while fulfilling our mission to protect investors and further the public interest in the preparation of informative, accurate and independent audit reports.

The proposed 2015 budget of $250.9 million represents a 7.9 percent increase ($18.5 million) over PCAOB's 2014 estimated spending of $232.4 million.

This expected growth is more realistic than that of the 2014 budget, which represented an increase of 15.1 percent over what was then the projected spending for 2013.

The proposed 2015 budget is 2.9 percent ($7.5 million) less than the approved 2014 budget.

This is the first year since 2006 that the Board's budget is less than the budget for the prior year.

However, the PCAOB was subject to the President's April 2013 sequestration order, which had the effect of reducing planned spending in 2014 by $6 million (from $258.4 million to $252.4 million).

The proposed 2015 budget is slightly less than this 2014 revised plan.

The current projected growth levels reflect the Board's remaining needs in furthering certain programs and initiatives that are underway, and in making improvements to our programs and operations.
During 2015, we will continue our interim broker-dealer inspection program, build on our relationships with foreign regulators to expand our

coverage of overseas inspections, integrate economic analyses into programs and activities, further develop a plan for the Center for Economic Analysis (CEA), and implement operational improvements to our administrative functions.

In addition, we will continue to build on our existing programs and activities through execution of recent initiatives.

Programmatic improvements begun in 2012 as Board "near-term priorities" have been integrated into the Board's strategic plan and budget this year, but some of those priorities continue to need additional work.

As I noted at last year's budget meeting, and it still remains true today, much work remains to be done for PCAOB to mature as a nimble and agile organization under a relatively stable size and structure.

I would like to comment on several of the Board's key initiatives.

Strategic Planning

First, I cannot overemphasize the importance of the planning and budgeting processes, which cover many months and involve the combined efforts of all PCAOB offices and divisions, the Board, and the Securities and Exchange Commission staff.

I commend all involved for the effort they made again this year and the thoughtfulness and dedication they contributed.

The PCAOB continues to make improvements to the planning and budgeting processes that have strengthened our controls and the outcome of our planning.

In addition, the staff has begun the process of considering budget assumptions in a more stable and lower-growth state for the organization.

This is an area that we will continue to refine and enhance to better integrate the strategic planning, policy-decision making, and budgeting processes, and the scheduling of these activities.

In addition, as I noted at last year's budget meeting, the Board needs to further develop and adopt strategic performance measures and benchmarks.

The staff has begun to consider programmatic performance metrics and process efficiencies with the assistance of the CEA.

I look forward to additional progress in the area of measuring PCAOB's progress and effectiveness in achieving its mission, including the goals and objectives articulated in the strategic plan.

Economic and Regulatory Analyses

Last year, the PCAOB established the CEA. I continue to support the functions of the CEA including

(1) rendering advice on how economic theory and analysis can be used to enhance the effectiveness of PCAOB programs,

(2) specifically dedicating resources to support economic analysis in standard setting and other rulemaking,

(3) fostering economic research on audit related topics, including the role and relevance of the audit in capital markets, and

(4) developing empirical tools for use in the PCAOB's oversight programs.

We still have work to do to finalize plans for these initiatives and fully realize their potential across PCAOB programs and activities.

Of urgency, in my mind, is the need to clearly delineate and define how the various activities within the CEA support the Board's mission and programs, including how the economists in the CEA will work with economists placed in the Office of Research and Analysis and the Office of Chief Auditor.

We need to ensure that the research projects being supported by the CEA through its annual conference and the work of its fellows will provide benefits in the areas of

(1) advancing research on the role of the audit in capital formation and investor protection and

(2) the effect of potential PCAOB actions intended to enhance the relevance and reliability of audits.

We also need to find ways to leverage the extensive body of research conducted by accounting and auditing researchers and continue our coordination with the American Accounting Association.

The budget request includes a total of $2.3 million to fund the activities of the CEA.

This amount is almost triple the amount that we anticipate spending for the CEA and its activities in 2014.

The staff currently plans to prepare, for the Board's approval, an activity plan and mission statement for the CEA that prioritize supporting the Board's primary functions.

In my view, the Board should hold the CEA's spending to a level below the requested budget amount until these planning activities are complete and the Board has approved the mission and activities of the center.

Progress on Near-Term Priorities

As I noted earlier, in 2012, the Board established six near-term initiatives that focused on improvements in the effectiveness of PCAOB's core mission activities.

As noted in the proposed 2014-2018 Strategic Plan, we have made notable progress on some of these priorities, and have used the progress to expand our goals in some areas.

For some of the initiatives, we still have significant work to accomplish, and I am pleased that the staff continues to work diligently not only on these areas, but on the expanded goals as well.

1. Improving the timeliness, content and readability of inspection reports.

The staff has cleared the backlog of older inspection reports and has set goals for the timely issuance of more current inspection reports.

In addition, the staff has begun to make some changes to inspection reports and is considering ways to improve the content and readability of inspection reports and general reports going forward.

To expand upon the original goal, we have significant opportunities in the area of providing timely and useful information to investors and our stakeholders regarding insights and results from our oversight activities.

We need to develop new approaches for disseminating summary information on inspection results as soon as possible during or after completion of an inspection cycle so that stakeholders have information about emerging risks and trends prior to the start of the next audit cycle.

In addition, PCAOB staff develops rich analyses related to specific risks related to auditing and general risks potentially impacting the audit profession.

Providing some of this information to the public on a summary basis would be helpful in promoting audit quality and protecting investors.

I look forward to continuing to work with the staff to on these important issues.

2. Improving the timeliness of remediation determinations and providing additional information about the PCAOB's remediation process.

The staff has cleared the backlog of older remediation determinations and related recommendations to the Board, and has set goals for the timely completion of current audit firm remediation submissions.

In addition, in 2013 the staff developed and published information about the quality control remediation process, including the criteria used to assess a firm's remedial actions.

Expanding on this original goal, the Board is planning to publish additional information about the remediation process, including information based on the staff's experiences with remediation activities across firms.

In addition, information about the staff's root cause analysis initiative and lessons learned in the application of economic analysis in PCAOB inspections activities should contribute to improved audit quality and stronger protection for investors.

3. Initiating a project to identify audit quality measures, with a longer term goal of tracking the application of such measures to global network firms and reporting on the results over time.

As I noted in last year's budget meeting and have articulated elsewhere, I fully support the development of a Board concept release on audit quality indicators.

The concept release will provide the public and all interested parties an opportunity to provide input into further analysis and future steps in the project.

This project should provide an insightful and valuable result, and I look forward to seeing the concept release issued in the near future.

4. Enhancing the PCAOB's processes and systems to improve the analysis and usefulness of PCAOB inspection findings, including a comparative analysis across firms and over time, in order to better understand audit quality in firms and better inform the PCAOB's standard-setting and other regulatory activities.

This project continues with a broad array of activities that include a number of enhancements to our information technology and operational processes.

These include enhancements to information systems in divisions and offices.

The Board has a remarkable opportunity to leverage the development and refinement of empirical tools and data analysis techniques of the CEA, Office of Research and Analysis, the Division of Enforcement and Investigations, and other offices to further enhance analysis to support our regulatory effectiveness.

The CEA has also made significant contributions to these efforts through its work to organize data for internal research purposes.

5. Enhancing the framework for the PCAOB's standard-setting process in order to improve the effectiveness of the process as well as the standard-setting project-tracking information provided to investors and the public.

Developing and finalizing a standard-setting framework will be important as we further integrate economic analysis into our standard-setting process.

Implementing a framework with analytical enhancements while moving forward on a significant standard-setting agenda represents a significant undertaking.

In that regard, I appreciate the interest and support of the SEC staff in addressing that challenge, and I note the interest in progress on PCAOB standard-setting expressed by the SEC Chair and Commissioners at the SEC's February 5, 2014 open meeting on the PCAOB's 2014 budget.

The Board plans to conduct a review of PCAOB's standard-setting function.

In my view, this review should be comprehensive, including the overall approach to standard-setting, identification of projects for the agenda, prioritization of projects, the process used for managing and monitoring projects, and potential performance measures.

6. Enhancing the PCAOB's outreach to, and interaction with, audit committees to constructively engage in areas of mutual interest, including auditor independence and audit quality.

The Board has taken a number of steps to reach out to audit committees to explore audit oversight issues and share information about PCAOB activities and inspection results.

These activities will continue in 2015 to extend our outreach to constructively engage in areas of common interest.

I have found my interactions with audit committees to be constructive and impactful.

I believe that ongoing interactions between PCAOB and audit committees is important, as the PCAOB and audit committees have mutual and complementary interests in advancing auditor independence and audit quality in promoting high quality, independent audits that protect investors and the public interest.

Other Key Initiatives

The proposed strategic plan and budget address a range of initiatives and activities intended to achieve three broad goals: effective oversight; constructive impact; and dedicated people.

I am pleased that our Chief Administrative Officer has consolidated a number of long-standing administrative needs into a comprehensive "transformation plan."

I have commented on many of these needs in the past two years, but I believe important elements include, in addition to those I mentioned earlier, the development of a strategic human capital plan, a regular periodic employee engagement survey, an enhanced diversity program, policies for flexible work arrangements, and additional non-monetary compensation incentives.

* * *

I believe that the budget we are voting on today appropriately reflects the Board's strategic priorities and resource needs for 2015 to fulfill our obligation to improve audit quality to protect investors and the public interest, while continuing the organization's evolution as a mature regulator.

In closing, I would like to join my fellow Board members in thanking the staff for their efforts in connection with the strategic plan and budget we are adopting today.

I would also like to thank SEC staff for their questions, comments, and feedback during the process of developing the strategic plan and budget.

Statement on Proposed 2015 Budget and Strategic Plan

Steven B. Harris, Board Member EVENT PCAOB Open Board Meeting
Washington, DC

Thank you Mr. Chairman. I support the Board's 2014-2018 Strategic Plan and the accompanying Budget.

The Board's proposed budget, as discussed in detail by the staff's earlier presentation for 2015, is $250.9 million.

This is equivalent to our revised spending plan for this year and reflects a decrease from the budget approved last year.

The 2015 budget reflects a compromise amongst Board priorities and resources.

I believe it represents a reasonable approach to meeting the goals spelled out in the 2014-2018 Strategic Plan and fulfilling our mandate "to protect the interest of investors and further the public interest in the preparation of informative, accurate and independent audit reports."

I want to touch on a number of accomplishments during 2014, and some of the priorities reflected in the Strategic Plan which I particularly support.

Maintaining a Focus on Auditor Independence and Audit Quality

In the Strategic Plan, the Board appropriately stresses the importance of continuing to focus on the independence, objectivity and professional skepticism of the auditor.

As framed in the Strategic Plan, I agree that we need to continue to carefully monitor and analyze the business models of the largest firms to ensure that audit quality and auditor independence are not compromised as the largest firms expand into additional lines of business.

Improving audit quality and ensuring auditor independence must remain top priorities as the firms grow their consulting and advisory services.

I further support the Board examining whether certain kinds of tax consulting services create conflicts of interests that may impair auditor independence.

The Strategic Plan makes clear that we will continue to hold auditors accountable for violations of our auditing standards and independence rules during inspections and as part of our enforcement oversight.

I likewise support the PCAOB's continuing its outreach to audit committees and constructively engaging with them in areas of common interest, including auditor independence, audit quality, and PCAOB inspection findings.

The PCAOB, as with other audit regulators around the world, remains concerned about the continued high number of observed audit deficiencies. Improving audit quality continues to be the underlying theme throughout the Strategic Plan.

The results of the findings of the 2013 Inspections Findings Survey of the International Forum of Independent Audit Regulators, issued in April 2014, are consistent with the findings of our own PCAOB inspectors — that the areas of fair value measurements and internal controls continue to have the highest number of inspection findings.

Standard Setting

As referenced in the Strategic Plan, the Board has an active standard-setting agenda.

For example, in August 2014, the PCAOB issued for public comment a Staff Consultation Paper on standard-setting activities related to auditing accounting estimates and fair value measurements.

I support this project as well as the Board's ongoing initiatives to improve our audit quality control standards.

In this regard, I continue to believe the Board should focus on the Failure to Supervise provisions of the Sarbanes-Oxley Act.

I further support the consideration of whether independent non-executives should be required on the governance boards of firms, something that is currently required in a number of jurisdictions.

I also support the Board's priority to identify audit quality indicators.

The goal is to promote competition based on audit quality amongst the firms and develop concise, summary reporting on the state of audit quality and other relevant information about auditing.

This important initiative should be of considerable value not only to the PCAOB, but to audit committees, auditors, investors, and companies alike. This issue is also of importance to regulators around the world.

Informative Audit Reports

Last December the Board published for comment a proposal to expand the current auditor's reporting model and in April 2014, we held a public roundtable on the subject.

This project, which involves examining possible changes to the auditor's report, is consistent with the Board's mandate to further "the public interest in the preparation of informative, accurate and independent audit reports."

Investors have been asking for an expanded auditor's report for a number of years now.

As the Strategic Plan notes, the PCAOB will continue to analyze insights gained from research, roundtables, consultation, economic analysis and public comment regarding potential changes to the model.

Regulators in other jurisdictions are likewise considering and, in fact, many have already required an expanded auditor's report.

For example, the European Parliament has voted to adopt a broad package of audit reforms for European Union countries that includes an expanded auditor's report.

The United Kingdom already requires such an expanded report.

The United Kingdom's move has been well received by investors, auditors and companies alike.

I believe we should move forward and finalize this project in the near future so that U.S. investors also are provided with a more informative and meaningful audit report.

Transparency

Likewise, we should adopt the Board's initiative on transparency and the identification of the engagement partner in the audit report.

I look forward to the Board successfully concluding this project as soon as possible in the new-year.

I note that such transparency is already common practice in much of the world.

Fraud Detection

The current proposal on the auditor's reporting model includes enhancements to clearly indicate the auditor's responsibilities for fraud.

Investors want, and expect the auditor to do more, to detect and expose fraud.

As the Strategic Plan notes, in the coming year, the PCAOB will work to "develop economic analysis that focuses on external economic factors that cause potential fraud pressures and risks."

This work will be done through the collaborative efforts of the PCAOB's Center for Economic Analysis and the Office of Chief Auditor.

This collaboration is part of the Board's Standards Division studying the auditors responsibility relating to fraud that began in 2012.

The discussion at last week's Standing Advisory Meeting, which dealt primarily with this topic, will inform the Board as it explores potential actionable ideas to enhance the effectiveness of audits in detecting financial statement fraud in 2015.

Economic Analysis

In early 2014, the PCAOB staff issued "Staff Guidance on Economic Analysis in PCAOB Standard Setting."

Under this guidance, each of the Board's proposed standards would address the following elements:

(1) the need for the proposed action;

(2) the baseline against which to measure the likely economic consequences of the proposed regulation;

(3) the alternative regulatory approaches considered; and

(4) an evaluation of the economic impact, including the benefits and costs—both quantitative and qualitative—of the proposed action and the main alternatives identified by the analysis.

The Board also considers whether the proposed action is in the public interest, whether it will protect investors, and if it promotes efficiency, competition and capital formation.

Integration of the Center for Economic Analysis to the Work of the Board

The Board's Center for Economic Analysis was formed earlier this year as well.

The center is designed to enhance the role of analysis in and of our programs, whether in providing perspectives on proposed actions or helping to structure post implementation reviews of our standards.

I am particularly interested in the center's project to catalogue the potential uses of the data the Board already has and explore what additional data we may need to enhance our inspection and standard setting processes, as well as to carefully consider the potential costs and benefits of the Board's programs.

Improving Data Analysis and Timeliness of Firm Remediation

Each year, the PCAOB strives to improve its oversight activities in many ways, including through an examination of our data.

For example, in 2014, the Division of Registration and Inspections continued to aggregate the findings in our inspection reports for large and small firms in a compendium for internal use and analysis.

Strengthening the analyses of our data and processes through the use of sophisticated information technology and data management tools, as envisioned in the Strategic Plan, will contribute positively to the effectiveness of our oversight programs.

With respect to the Board's remediation determinations, I support our efforts to improve the timeliness of the Board's remediation determinations which the Strategic Plan notes is one of the Board's near term priorities.

I also support the Board providing additional information about the PCAOB's remediation process to the investing public and audit firms; focusing on improving the timeliness, content and readability of inspection reports; and improving the firms' root cause analysis, where appropriate.

Broker Dealer Audits

With respect to the Board's broker-dealer program, I believe we are making considerable progress in developing a regulatory and operational infrastructure to carry out our oversight authority for broker-dealer auditors as authorized under the Dodd-Frank Act.

International Outreach

On the international front, I would like to acknowledge the PCAOB's continued work with our international regulatory counterparts with the goal of achieving greater access to cross-border inspections.

In 2014, the PCAOB entered into cooperation agreements with Sweden and Denmark, bringing the total number of cooperative agreements reached with non-U.S. auditor oversight authorities to 18.

I view this as a significant achievement and would like to commend Chairman Doty, and our Office of International Affairs, under the leadership of Bruce Wilson, for the Board's success in this area.

The PCAOB further reinforces international cooperation through its participation and leadership in the International Forum of Independent Audit Regulators, which brings together independent audit regulators from some 50 jurisdictions around the world.

The Strategic Plan also appropriately focuses and highlights the Board's ongoing efforts on reinforcing quality control at the global network firms.

Budgetary Considerations

In considering and finalizing the Board's 2015 budget — which now must be approved by the Securities and Exchange Commission -- I believe the

Board has carefully assessed, and continues to assess, the growth of the PCAOB with an eye towards reaching a steady-state level in its budget.

The Board understands the need to budget to reasonably achievable activity and provide justification of its spending, and to carefully oversee its divisions and offices.

I believe this budget responsibly represents that effort.

Before closing, I join you, Mr. Chairman, and the other Board members in acknowledging and thanking the staff for all their hard work on the budget and strategic plan.

Most people are unaware of how many people contribute to the final product that is before us today. I want to particularly thank Suzanne Kinzer, our Chief Administrative Officer, and Bill Wiggins, Jim Hearn, Amy Hargrett, Yoss Missaghian, and Bobbie Reichert.

Also, Phoebe Brown, our Corporate Secretary. I also want to acknowledge the assistance of the staff at the SEC on the development of both the budget and strategic plan.

Emergency Preparedness: Are We Ready For A 21st Century Hugo?

Written testimony of FEMA Office of Response and Recovery Acting Deputy Associate Administrator Robert Fenton for a House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency field hearing titled "Emergency Preparedness: Are We Ready For A 21st Century Hugo?"

Introduction

Chairman Duncan, Ranking Member Barber, and other distinguished members of this Subcommittee, thank you for the opportunity to testify today on behalf of the Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA).

I am Robert J. Fenton, and I currently serve as the acting Deputy Associate Administrator for FEMA's Office of Response and Recovery.

Over the years, FEMA Headquarters and its regional offices have worked closely with state, local, tribal and territorial governments across the country, and with faith-based organizations, to develop catastrophic, worst-case scenario plans that are flexible and scalable for incidents of all magnitudes.

FEMA's ongoing partnerships with states allow coordination and collaboration with the "Whole Community" to plan and prepare for a range of disaster events.

As this subcommittee is aware, this year marks the twenty-fifth anniversary of Hurricane Hugo.

Its impact on the state of South Carolina and surrounding states was a harbinger for even more destructive and costlier hurricanes to hit our shores — including Hurricanes Andrew, Katrina, Rita, Wilma, and Sandy.

When Hurricane Hugo hit the Southeastern region of the United States, FEMA was a relatively young agency — ten years in existence — with limited experience, exposure, and practice with catastrophic disasters.

Today, FEMA is a very different organization than it was twenty-five years ago.

With more statutory authorities, a better skilled, experienced and agile workforce, a keen focus on a whole community approach to emergency management, and the advent of social media and other technologies, FEMA is transforming the way in which our nation prepares for, responds to, and recovers from all hazards.

Hurricane Hugo

Hurricane Hugo made landfall just north of Charleston, South Carolina, at midnight September 21, 1989, as a Category 4 hurricane with 135 mph winds, and rolled through South Carolina on a northwest path.

The storm's strong winds extended far inland and storm surge inundated the South Carolina coast from Charleston to Myrtle Beach.

Hours later, the storm tore through much of North Carolina.

It was the strongest hurricane on record to hit South Carolina, and the second strongest hurricane — since reliable records began in 1851 — to hit the Eastern seaboard north of Florida.

More deadly and destructive than Hurricane Hugo's 135 mph winds were the surging tides accompanying landfall.

The combination of high tide, the tidal surge preceding Hugo and waves generated by the storm inundated a wide area of coastal plain.

In Charlotte, North Carolina, hundreds of miles inland, residents lost power for up to 18 days as thousands of trees, broken limbs and debris severed power lines.

In South Carolina alone, FEMA provided $70 million to individuals and families for housing and other disaster-related expenses and $236 million for debris removal, public utility and infrastructure repair or replacement and emergency protective measures.

According to the National Weather Service, Hurricane Hugo was the costliest hurricane on record to hit the United States at the time.

How FEMA is Transforming in the 21st Century

I. Whole Community Approach to Emergency Management

Hurricane Hugo, like many other disasters, draws our communities even closer together and catalyzes the actions of not only our federal, state and local governments, but also the private sector, ordinary citizens, and many other sectors of society.

Thus, preparedness is a shared responsibility, and it calls for the involvement of everyone in preparedness efforts.

By working together, everyone can make the nation safer and more resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics.

In addition, FEMA created a "seat at the table" for the private sector through our Private Sector Representative Program.

This is a 90-day private sector rotation that was started in 2012.

To date, we have had representation from nine companies, one academic institution and one NGO. Regions have begun implementing the program as well.

Wells Fargo currently has an employee as the Private Sector Representative, working with Regions IX and X.

The three core principles of whole community — understanding and meeting the actual needs of the whole community, engaging and empowering all parts of the community, and strengthening what works well in communities on a daily basis — provide a foundation for pursuing a whole community approach to emergency management through which security and resiliency can be attained.

In 2007, FEMA created a Private Sector Division in the Office of External Affairs and put private sector liaisons in each of the FEMA ten regions.

Private sector specialists at headquarters, the regions and joint field offices serve as a gateway to private sector engagement and integration.

Furthermore, the division also runs the National Business Emergency Operations Center (NBEOC), to facilitate public-private information sharing and situational awareness with operational partners during major disasters.

The NBEOC is a virtual organization and currently has 377 members from both the private and public sectors.

Building on our whole community efforts, in 2012, FEMA created a "seat at the table" for the private sector through our Private Sector Representative Program. To date, we have had representation from nine companies, one academic institution and one non-governmental organization (NGO).

FEMA regions have begun implementing the program as well – including Region IV which supports the Southeastern region, including the state of South Carolina.

In July 2013, FEMA launched a new program known as Tech Corps.

The Tech Corps Program is the product of Senator Ron Wyden's vision for a way to integrate trained, corporate technology volunteers into disaster response at the state, local, tribal and territorial levels – whom they support directly.

In short, by engaging and working with the whole community, everyone can make the nation safer and more resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics.

Collectively, our nation can achieve better outcomes in times of crisis, while enhancing the resilience of our communities.

II. Building on National Preparedness Efforts

FEMA's planning efforts are centered on our preparedness policy and doctrine, which leads to coordinated catastrophic planning that relies on a shared understanding of threats, hazards, capabilities, processes, and ultimately, the value of being prepared.

This Administration remains steadfast in its commitment to strengthening the security and resilience of the United States; and, we continue to become more secure and better prepared to prevent, protect against, mitigate, respond to, and recover from the full range of threats and hazards the nation faces.

We plan, organize, equip, train, and exercise better, resulting in improved national preparedness and resilience.

Much of this progress has come from leadership at the state, local, tribal and territorial levels, fueled by FEMA's grant programs.

Over the past ten years, DHS has provided state, local, tribal, and territorial governments with billions of dollars in grant funding.

As a nation, we have built and enhanced capabilities by acquiring needed equipment, funding training opportunities, developing preparedness and response plans, and continuing to conduct exercises that help build relationships across city, county, and state lines.

For instance, in the last four years alone, FEMA has awarded approximately $313 million for hurricane/high wind mitigation projects.

These project types include safe rooms for first responders and critical staff; structural retrofits that provide high wind protection for vulnerable buildings and critical infrastructure.

In addition, FEMA has provided funding for emergency power generation at critical facilities; weather warning system enhancements; training and other support for building code officials, and community education efforts.

Although FEMA's grant funds represent just a fraction of what has been spent on homeland security across the Nation, these funds and the development of capabilities they have made possible, have helped change the culture of preparedness in the United States.

Presidential Policy Directive 8 (PPD-8)

In March 2011, President Obama signed PPD-8, which describes the nation's approach to national preparedness. PPD-8 aims to strengthen the security and resilience of the United States through the systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber incidents, pandemics, and catastrophic natural disasters.

PPD-8 defines five mission areas – prevention, protection, mitigation, response, and recovery – as part of a continuum of interrelated activities and requires the development of a series of policy and planning documents to explain and guide the nation's efforts in helping to ensure and enhance national preparedness.

PPD-8 created the National Preparedness System (NPS), a cohesive approach that allows us to use the tools at our disposal in the most effective manner and to monitor and report on progress being made in national preparedness.

Moreover, the NPS was designed to help guide the domestic efforts of all levels of government, the private and nonprofit sectors, and the public to build and sustain the capabilities outlined in the national preparedness goal.

And finally, NPS helps to articulate how well prepared we are by setting a goal, establishing baseline capabilities, setting common and comparable terminology, measuring capability gaps, and assessing our progress toward filling them.

III. Catastrophic Planning and Preparedness

Understanding the critical importance of catastrophic preparedness, FEMA is also leading substantial response planning, including the development of plans across the Federal government for catastrophic incidents; future operations for potential/actual incidents; regional planning for all-hazards events; and evacuation and transportation planning.

There are also special programs focused on planning for chemical, biological, radiological, nuclear, and explosives (CBRNE) hazards to communities throughout the Nation.

In addition to these planning efforts, FEMA coordinates closely with our federal partners in many ways on other efforts in preparing for disasters, including the development of pre-scripted mission assignments, interagency agreements, and advanced contracts for commodities.

These partnerships are essential to FEMA's ability to carry out its mission by leveraging the full capacity of the federal government.

IV. Critical FEMA Authorities Post Hurricane Hugo

Post-Katrina Emergency Management Reform Act (PKEMRA) of 2006

In addition to building on our Whole Community efforts over the years and creating more robust and better informed catastrophic plans, Congress has

also played an instrumental role in transforming FEMA into a more effective and efficient agency.

The importance of PKEMRA to the emergency management community is significant.

PKEMRA provided FEMA clearer guidance on its responsibilities and priorities, and the authorities and tools we needed to become a more effective and efficient agency, and a better partner to state, local, territorial, and tribal governments.

PKEMRA also continues to give us the authority needed to lean forward and leverage the entire community in response and recovery efforts.

This Whole Community approach emphasizes the importance of working with all partners to successfully prevent, protect against, respond to, recover from, and mitigate all hazards.

Sandy Recovery Improvement Act of 2013 (SRIA)

In January 2013, Congress passed and President Obama signed SRIA into law, authorizing several significant changes to the way FEMA delivers disaster assistance.

SRIA is one of the most significant pieces of legislation impacting disaster response and recovery since PKEMRA and builds upon the Robert T. Stafford Emergency Relief and Disaster Assistance Act.

SRIA, and the additional authorities it provides, is aiding recovery efforts associated with recent disasters such as Hurricane Sandy and the floods that impacted the state of Colorado.

SRIA's various provisions are intended to improve the efficacy and availability of FEMA disaster assistance and make the most cost-effective use of taxpayer dollars.

One clear example of SRIA's effectiveness in use of taxpayer dollars is the Public Assistance Permanent Work Alternative Procedure provision which provides substantially greater flexibility in use of federal funds for Public Assistance applicants and far less administrative burden and costs for all parties – if applicants accept grants based on fixed, capped estimates.

To date, FEMA has agreed to fund billions in public assistance permanent work alternative procedure projects in states such as New York and Louisiana.

Another SRIA provision, National Strategy to Reduce Costs on Future Disasters, called on FEMA to submit recommendations for the development of a national strategy for reducing costs, loss of life, and injuries associated with extreme disaster events in vulnerable areas of the United States.

As such, On September 6, 2013 FEMA submitted this National Strategy report to Congress recommending ways in which multiple areas could be further explored during the development of a national strategy within the following themes:

(1) Engage in a Whole Community Dialogue and Build upon Public-Private Partnerships,

(2) Enhance Data-Driven Decisions;

(3) Align Incentives Promoting Disaster Cost Reduction and Resilience

(4) Enable Resilient Recovery and

(5) Support Disaster Risk Reduction Nationally.

All told, these recommendations offered examples of areas that would need much greater discussion and research to develop into a strategic and actionable path forward.

The implementation of cost reduction and cost avoidance strategies will require commitment and investment by the whole community to achieve the potential long-term savings and impact.

V. The Power and Promise of Social Media and other technologies in Emergency Management for the 21st Century

The advent of social media and other technologies has helped to transform FEMA into an agency that is more in tune with the needs of our citizens, especially during times of crisis.
FEMA's approach to emergency management recognizes that individuals, families and communities are our greatest assets and the keys to our success.

In order to fulfill our mission, we must work together as one team — this notion is, again, at the heart of our whole community approach to emergency management.

Social media is imperative to emergency management because the public uses these communication tools regularly.

Rather than trying to convince the public to adjust to the way we at FEMA have traditionally communicated, we have adapted to the way the public communicates, leveraging the tools they use on a daily basis.

Millions of Americans use social media every day to check in on friends and family, learn about current events, and share their experiences.

FEMA uses social media to be part of this ongoing dialogue and meet people where they are, using tools and platforms with which they are already familiar.

FEMA also uses social media and other digital methods to communicate because as we have seen, information can lead to action.

Our goal is for our safety-related information to have a real-world impact — to inspire actions that lead to more resilient families and communities. If someone sees a preparedness or safety tip from FEMA, the goal is that it will inspire them to prepare themselves as well as empower them to tell a friend how to be more prepared or where to find help.

Lastly, social media and emerging technologies allow us to reach more people more quickly during disasters, when they need accurate, timely and authoritative information that helps ensure the protection of their life or livelihood.

With one click of the mouse, or one swipe of the smartphone screen, FEMA and its whole community partners can share a message to thousands of people and have a tangible impact.

These capabilities did not exist twenty five years ago when Hurricane Hugo hit the Southeastern coast of the United States.

Conclusion

Finally, although FEMA has made important strides and progress over the years since Hurricane Hugo, we still have much work to do.

I am confident that with the additional authorities Congress has provided, an emphasis on a Whole Community approach to emergency management, a growing and more skilled work force, social media, and lessons learned from disasters over the years, FEMA will continue to be an agile and innovative Agency for many years to come.

Again, thank you Chairman Duncan for providing me this opportunity to appear before you today to discuss emergency preparedness for the 21st century.

I look forward to answering questions you or other members of this Subcommittee may have.

PCAOB Auditing Standard-Setting Update

Jay D. Hanson, Board Member
AICPA Conference on Current SEC and PCAOB Developments
Washington, DC

Good Afternoon,

Thank you for the opportunity to be here with you today.

I have attended this conference as a participant or speaker for many years, and I am always impressed with the quality of the speakers and the broad audience reached by this conference.

With thousands of participants attending here in Washington, participating in other cities, or listening on-line, this event reaches one of the largest audiences of accountants and auditors every year.

You already heard yesterday from the PCAOB's Chairman, Jim Doty, and you will hear from a number of other PCAOB speakers during this conference, including our Chief Auditor and the Directors of our Inspections Division, Enforcement Division and Office of Research and Analysis.

Between all of us, you will hear a lot about what we are up to at the PCAOB, and I will try to not duplicate the information they will provide.

But one thing you will hear from all of us is our disclaimer, which requires me to say that the views I express today are my personal views and do not necessarily reflect the views of the Board, any other Board member, or the staff of the PCAOB.

Turning to the substance of my remarks today, I would like to discuss today my perspective on several concepts important to the PCAOB, many of which others have mentioned already at this conference.

They all happen to begin with the letter "R": Relevance, Reporting, Remediation and Root Cause.

Relevance

2001 was a dark year. Of course, no one can forget the horrific events on September 11, 2001, including the loss of life, the terror in America, and the uncertainty of the future world order.

But that fall also marked the start of a historic decline in the confidence in public company financial reporting and the audit profession.

Enron's first press release, announcing unprecedented losses and billion dollar charges against its balance statement, was issued in October 2001.

The subsequent cascade of restatements at Enron and elsewhere, and the discovery of extensive fraudulent financial reporting, marked a historic low point for the accounting and auditing professions.

Actions by Congress in 2002, resulting in the Sarbanes-Oxley Act of 2002 (SOX or Act) and the creation of the PCAOB, were a reaction to the crisis and necessary to reform behavior and restore confidence in the capital markets.

In contrast to more recent reform legislation, referenced by Commissioner Gallagher in his remarks yesterday, SOX hit the mark on many fronts.

The Act drove three primary developments: Changes in corporate governance giving the audit committee explicit responsibility for auditor oversight; new requirements for management to certify the financial statements and controls; and a new world for auditors who were made subject to PCAOB oversight.

Taken together, these changes have made a tremendous difference.

The PCAOB has now been in operation for almost 12 years.

Through the issuance of 18 new auditing standards and revisions to many others, over 2,000 inspections, and more than 80 enforcement actions, the Board has made substantial, relevant contributions to improving public company auditing.

Auditors have become increasingly aware of their obligation to investors and the public.

Audit committees have significantly upped their game in overseeing auditors.

And while inspection findings indicate that auditors continue to struggle in a number of key areas, firms have made substantial investments to understand the causes of ongoing deficiencies and to drive improvements in their work.

Yet, I am often asked whether we have struck the right balance to drive positive changes while avoiding the imposition of unreasonable burdens.

That is a question that all of us at the Board should regularly ask ourselves.

You will hear more tomorrow about our inspection findings, which continue at a rate that no one finds acceptable.

Of course, the PCAOB has improved at identifying potential problem areas and scoping inspections accordingly.

Our inspections of the largest firms are primarily risk based and review audit work in the most difficult and subjective areas.

At the same time, firms are changing the way they carry out the work, including, for example, through increased aggregation and analysis of large quantities of data.

Will there come a time when audit practice has improved, or evolved, to the point that we should change our approach to inspections or their scope?

Clearly, audit quality is not yet where we want it to be, but, in order for the PCAOB to remain effective and relevant, we must continually scrutinize our work and its results, in order to allow us to evolve and continue to contribute to the improvement of the audit profession even as conditions change.

Our standard setting process, which our Chief Auditor, Marty Baumann, will talk about in a few minutes, also is more rigorous than ever.

We have issued some fundamentally important standards and amendments, including those relating to the audits of internal controls and those governing risk assessments, related parties, audit committee communications and others.

But more remains to be done, and the Board is committed to improving our standard setting process, where possible, to make it more efficient and effective.

Several speakers yesterday, including Chief Accountant Schnurr, Deputy Chief Accountant Croteau, and Commissioner Gallagher questioned whether the PCAOB standard setting process could be improved to result in more timely output of new performance standards.

I look forward to working with the SEC staff on a review of our processes, including by taking a look at some fundamental issues such as how topics are added to or removed from our standard setting agenda and how they are prioritized.

Our standard setting program now also explicitly incorporates economic analysis.

We have hired several economists to help us tackle this important work, but we all have a lot left to learn.

For example, the concept of "information asymmetry" seems to permeate much of our economic analysis.

In trying to relate this concept to the world of auditing and audit reports, I think of an analogy to when management evaluates a target for an acquisition.

The more a potential acquiring party knows about a target (for example through extensive due diligence), the better it is able to price the acquisition.

A set of audited financial statements alone usually would not be sufficient due diligence.

Investors tell us that they rely on the audit as part of their due diligence when evaluating an investment.

Thus, the more investors can learn from and rely on the financial statements and the more they learn about important audit issues, the better they can price their investment.
We will continue to refine our thinking on this and other important economic concepts with the goal of driving the right changes in audit practice without imposing the wrong costs.

Few would argue that the PCAOB has not been an important contributor to the improvements in financial reporting and auditing that have largely restored the confidence in the capital markets that was lost in 2001 and 2002.

But our work is not done, and the tough challenge ahead, I believe, will be how to continue to make relevant improvements, at justifiable costs, as both the business world and auditing continue to evolve.

Reporting

One important aspect of our work that is directly related to our effectiveness and our relevance is the reporting of our findings.

In addition to individual inspection reports, the Board issues summary reports aggregating inspection findings or highlighting particular trends, as well as staff practice alerts regarding frequently observed auditing deficiencies.

Our staff has been working on improving our individual firm inspection reports, which are our primary means for communicating our findings.

We are issuing reports on a more timely basis.

We have started including detailed references to the auditing standards that give rise to the deficiencies.

This is a great start, but I believe we can and should do even more to make the individual reports more meaningful and easier to understand, including by providing more context around our findings.

As a Board member, I can look at much of the detail that supports each finding cited in the public report, and I can see the trends from year to year for each firm and between firms.

I know which audit areas in a given year were the source of the most deficiencies, and I have the context of which findings involved violations by individual auditors of the firms' policies versus those which involved inadequate firm guidance.

I know why we picked an issuer, its size and industry, and what audit areas we chose to review, and I can see whether the audit was a "train wreck," a "near miss" or a one-off deficiency that will be relatively easy to address.

Some of this context, I believe, would be helpful to our readers as well and I believe we should find a way to report it.

Another challenge we face in connection with our reporting is the balance between timeliness and accuracy.

We recently met with an audit committee chair who articulated a common sense request — to share broadly the trends we are seeing in our current-year inspections, and potential audit risks, before the individual firm inspection reports are issued.

This audit committee member wants to be able to engage his auditors about potential problems at a time when those issues are still fresh and potentially relevant to his auditors' current work, rather than one or two audit cycles later, after our inspection report has been issued.

It is hard to argue with such a request from an audit committee member who is trying his best to exercise rigorous corporate governance, and we need to think about how we might be able to respond.

Likewise, we have made some improvements in our general inspection reports, which aggregate findings or report on specific issues or trends.

In recent years, we have added executive summaries to these reports to try to provide, up front, a clear message about what we are finding and what it may mean to firms, audit committees, investors and others.

I am hoping that we can continue to improve these reports, including by issuing them more timely and by fleshing out the reports to provide more analysis and context about our findings and relevant trends.

In carrying out our mission, we gain valuable information about audit firms and practices.

We see and report on audits that did not meet our standards in some way.

We also inspect a substantial number of audits each year, in firms large and small, where the work was done well, and we have no deficiencies to report.

I consider all the insights we gain as valuable resources that can and should be shared with our stakeholders.

I would like to see us use all of our resources to further improve audit quality.

Remediation

One of the most important ingredients for audit quality is the firm-wide quality control system designed to provide assurance that firm personnel comply with applicable professional standards and the firm's standards of quality in performing audits.

Therefore, one of the most effective ways to improve audit quality is to successfully remediate deficiencies in that quality control system to eliminate systemic problems with audit engagement performance.

The Act provided an incentive to do just that, by requiring firms to remediate quality control deficiencies identified by Board inspections within twelve months of the date of the inspection report, or risk publication of any deficiencies that are not timely remediated.

As the Board observed early on in its existence, this requirement "rested on the hypothesis that firms could be genuinely motivated by the prospect of keeping the Board's quality control criticisms confidential."

In 2006, along with issuing a Board release describing the Board's process for determinations regarding remediation, the Board issued a general report, discussing its observations of the firms' initial implementation of the remediation requirements.

Since then, the PCAOB and registered firms have gained several years of additional experience with the remediation process.

With respect to the vast majority of quality control deficiencies, firms took appropriate remedial steps.

The Board has, however, made public some or all of the quality control weaknesses or deficiencies of over 150 firms, including some that provided no response to the Board to describe their remedial efforts.

Of the largest six public accounting firms in the U.S. which are members of global firm networks, five have been subject to publication by the Board of one or more quality control deficiencies as a result of a Board determination that these deficiencies were not timely remediated.

Having evaluated firm remediation efforts for a number of years, the PCAOB last year issued staff guidance describing the considerations that the inspections staff has identified as relevant to its recommendations to the Board concerning the sufficiency of firms' remediation efforts.

This guidance set forth a series of criteria used by the staff to formulate its recommendation to the board and is intended to help firms better tailor their remediation efforts to the Board's expectations.

We are hoping to provide additional information about the remediation process and the Board's determination, as well as a follow-up general report to describe some of the remedial actions firms have taken more recently, and how effective those steps were deemed by the Board and staff.

Root Cause

But before a firm can begin to design and implement appropriate remedial actions, the firm has to ask itself: What is the problem that needs to be solved?

If additional training or a new practice aid, tool or policy is put into place but does not address the real reason for the deficiency, much effort will be wasted, and audit quality is unlikely to improve.

As a result, our Inspections Division has been working with firms, particularly the largest firms, to facilitate a root cause analysis of the underlying causes of their quality control deficiencies.

Root cause analysis is a widely used concept in various industries to analyze and understand problems as a way to develop solutions that address the underlying problem rather than symptoms of the problem.

Our Inspections staff has begun to analyze audit deficiencies using causal analysis techniques, involving many complex interrelationships between each cause and effect that resulted in an audit quality event.

Likewise, we are urging firms to implement rigorous processes to understand the causes and effects contributing to their systemic quality control deficiencies, allowing them subsequently to take effective actions to address those deficiencies.

The other side of the coin is trying to understand what firms do well, or, put another way, conducting root cause analysis of positive audit quality events.

In order to drive improvements in audit quality, we need to understand not only what auditors do wrong, but also what they do right or how they successfully tackle difficult challenges.

Although our inspection program is designed to test for compliance with auditing standards and other applicable rules, and therefore traditionally has focused on identifying poor audits, rather than good audits, we have made inroads into trying to understand better what factors contribute to high audit quality.

To that end, our Inspections Division has begun to identify audits that were performed well and to conduct root cause analysis to determine what sets those audits apart from others.

Analyzing positive events may enable firms to articulate what is needed to again achieve those positive events and result in improved processes and work flows.

At the same time, our Office of Research and Analysis has been working on identifying useful audit quality indicators, including certain "input" or "process" indicators that may shed light on what activities by auditors lead to positive audit quality events.

This analysis will leverage root cause analysis work by the Inspections Division and audit firms, and we hope that we ultimately will be able to communicate information about activities and processes that will help auditors perform effective, high quality audits on a consistent basis, as well as equip audit committees, investors, and others with information to aid in their evaluation of audits.

With that, let me thank you again for listening, and I will now turn to Marty Baumann to provide a little more detail about what is happening in the area of PCAOB standard setting.

Sarbanes Oxley Compliance Professionals Association (SOXCPA)

As our association becomes larger, you can explore some new opportunities.

This is what we offer:

1. Membership - Become a standard, premium or lifetime member.

You may visit:
www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Subscribe to receive (at no cost) Sarbanes-Oxley related alerts, opportunities, updates and our monthly newsletter:
http://forms.aweber.com/form/30/1922348130.htm

3. Training and Certification - Become a Certified Sarbanes Oxley Expert (CSOE).

You must follow the steps described at:
www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to your needs.

4. Authorized Certified Trainer, Certified Sarbanes Oxley Expert Trainer Program (SOXCPA-ACT / CSOET) - Become an ACT. This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.
To learn more:
www.sarbanes-oxley-association.com/SOXCPA_Authorized_Certified_Trainer.html

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.