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, October 2022

Dear members and friends,

The Federal Reserve Board has invited comment on updates to operational risk-management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board.

FMUs provide essential infrastructure to clear and settle payments and other financial transactions upon which the financial markets and the broader economy rely to function effectively.

The proposed updates generally provide more specificity to the existing requirements.

The broad operational risk, technology, and regulatory landscape in which FMUs operate has evolved significantly since the Board last updated its risk management requirements for FMUs in 2014.

New challenges have emerged, such as the global pandemic and cyber events, while new technological advancements may improve resilience. The

proposed changes would promote effective risk management in this rapidly evolving risk environment.

"In light of the rapidly evolving risk landscape, the proposed changes will help ensure that key financial market utilities operate with a high level of resilience and remain a source of strength for the financial system," said Vice Chair Lael Brainard.

The proposal addresses four key areas: incident management and notification; business continuity management and planning; third-party risk management; and review and testing of operational risk management measures.

For example, the proposal would explicitly require FMUs to establish an incident management framework and would emphasize the need for FMUs to continue to advance their cyber resilience capabilities. The proposed updates are largely consistent with existing measures that FMUs take to comply with the current requirements.

Comments on the proposed changes must be submitted within 60 days from the date of publication in the Federal Register.

For media inquiries, email media@frb.gov or call (202) 452-2955.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220923a.htm

Technology and Talent - Audit Quality Challenges in the 21st Century

Christina Ho, PCAOB Board Member,
Deloitte PPD Seminar, Washington, DC

Thank you for the introduction. It is a pleasure to be here today and since you gave me the luxury of picking my own topic, I thought I would share my perspectives on audit quality challenges in the 21st century. The views that I express here are my own and do not necessarily reflect the views of other PCAOB Board members or staff.

Hindsight is 20/20

In July of this year, we celebrated the 20th anniversary of the Sarbanes-Oxley Act of 2002, affectionately known as "SOX". You may recall that the birth of SOX started with egregious corporate scandals.

The first was Enron, a corporation that appeared to be a reputable energy company at the time. The company's leadership created fictitious holdings, used special purpose entities to hide their debt and toxic assets, and falsified accounting records. Eventually, Enron filed for Bankruptcy in 2001, tumbling its share price from its height at $90.75 to a mere $.26 cents.

This scandal spurred not only the demise of the company but also its auditor, Arthur Anderson, and eradicated the life savings of numerous hardworking employees and investors who had the utmost confidence in the company's financial position.

Following suit in 2002 was another large accounting scandal, resulting in the bankruptcy of WorldCom, the 2nd largest long-distance telephone company at the time.

Both Enron and WorldCom intentionally "cooked the books," and again, Arthur Anderson turned a blind eye at WorldCom for inflating profits.

Given these extensive financial scandals, the federal government implemented sweeping reform by enacting SOX with bipartisan congressional support.

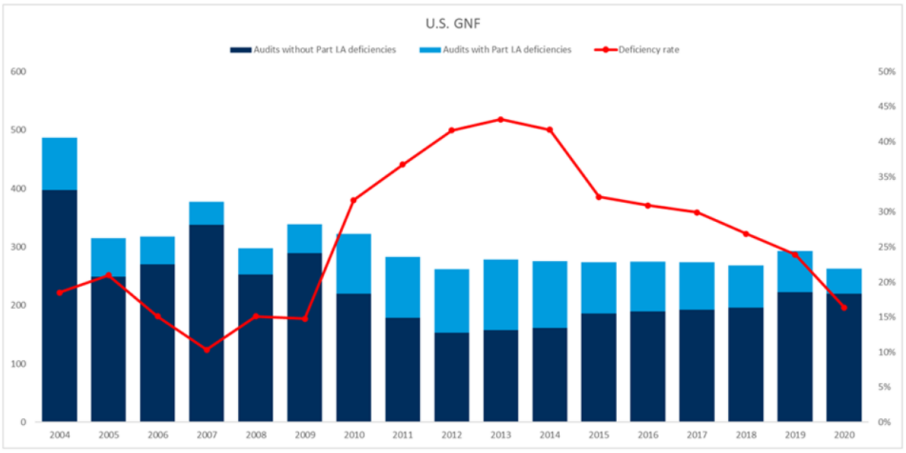
With the enactment of SOX came the beginning of the PCAOB and the end of more than 100 years of self-regulation by the accounting profession.

As a newly formed independent regulatory and oversight body, the PCAOB had its growing pains during the initial years and has evolved in maturing its programs throughout the past 20 years.

Today, the PCAOB has almost 1,700 registered firms, including U.S. and non-U.S. registered firms. In relation to foreign registered firms, most recently on August 26, 2022, PCAOB Chair Williams announced that the PCAOB had signed an agreement with People's Republic of China authorities, which is the first step toward opening access for the PCAOB to inspect and investigate completely registered public accounting firms in mainland China and Hong Kong.

Prior to her August 26, 2022 announcement, Chair Williams provided remarks on the celebration of the SOX 20th anniversary on July 28, 2022.

In that speech, Chair Williams shared that the PCAOB has completed over 4,300 firm inspections in 55 countries, including reviewing more than 15,000 audits of public companies and over 1,000 broker-dealer engagements.

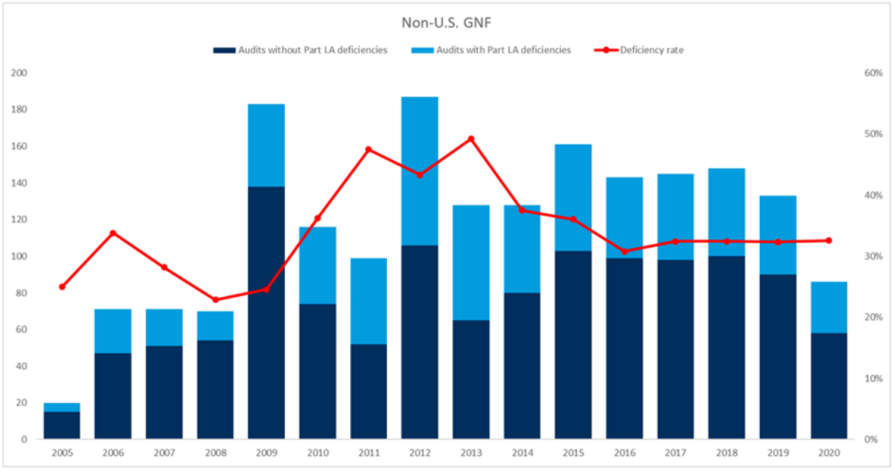


Source: PCAOB (Tables Contain Aggregated, Anonymized, and Rounded Publicly Available Data)

To provide historical context, I would like to share some high-level trends of the deficiency rates for both the U.S. and Non-U.S. Global Network Firms (GNF) since the inception of our Inspection program.

As illustrated, the Part I.A findings deficiency rate for U.S. GNFs in 2004 was about 18%, which trended downward through 2007 to about 10%, rising to over 40% at the peak in 2013, then settled back down to about 16% in 2020. The deficiency rate is the ratio of audits with findings relative to the total number of audits (with and without findings) reviewed by the PCAOB Inspections division.

For Non-U.S. GNFs, the trending is similar, starting at about a 25% deficiency rate in 2005, slightly down to below 25% in 2008, up again to nearly 50% in 2013, then landing at about 33% in 2020.



Source: PCAOB (Tables Contain Aggregated, Anonymized, and Rounded Publicly Available Data)

To read more: https://pcaobus.org/news-events/speeches/speech-detail/ho-technology-and-talent-audit-quality-challenges-in-the-21st-century

PCAOB Chair Williams Delivers Remarks at CII Fall Conference

Thank you, Jeff [Mahoney] and everyone at CII for inviting me to be a part of your conference. And thank you for the work you do on behalf of Main Street investors from firefighters to schoolteachers.

Before we begin, I want to issue the standard disclaimer that the views that I express here are my own and are not necessarily the views of the other Board Members or the PCAOB staff.

China

The PCAOB inspects and investigates registered public accounting firms in more than 50 jurisdictions around the world. These inspections and investigations are two of the most important tools we use to protect investors.

But, for more than a decade, our access in mainland China and Hong Kong has been restricted, potentially putting investors at risk.

On August 26th, we took a first step toward opening up our access in mainland China and Hong Kong when I joined the China Securities Regulatory Commission and the Ministry of Finance of the People's Republic of China in signing the most detailed and prescriptive agreement we have ever reached.

On paper, the agreement guarantees the PCAOB complete access to inspect and investigate any firm we choose, with no loopholes and no exceptions.

Specifically, there are three key provisions.

One: The PCAOB has sole discretion to select the firms, audit engagements and potential violations it inspects and investigates – without consultation with, nor input from, Chinese authorities.

I have said before, and I will say again: voluntarily delisting is not an escape hatch for avoiding PCAOB scrutiny. Our inspections and investigations are retrospective.

If a company delists this year, we still need to know whether wrongdoing occurred in previous years.

Two: Procedures are in place for PCAOB inspectors and investigators to view complete audit work papers with all information included and for the PCAOB to retain information as needed.

Any interference with our ability to retain information as needed is a dealbreaker.

Three: The PCAOB has direct access to interview and take testimony from all personnel associated with the audits the PCAOB inspects or investigates.

Now we must find out whether what we have on paper holds up in practice.

I want to be very clear: the time for negotiations is over. The agreement has been signed. And it must be followed completely.

Last week, PCAOB teams began arriving in Hong Kong where they will conduct inspections of firms in both mainland China and Hong Kong.

As with all inspections, they will look at various factors, including the audits of specific selected companies and the overall quality control systems of the audit firms themselves. They will review audit opinions that firms sign directly, and audit work those firms perform on behalf of others.

I have been asked many times how long this process will take. The answer depends in part on China's cooperation.

Our team will work swiftly and thoroughly. China must cooperate just as swiftly and thoroughly in return.

One thing is certain: by the end of this year, the PCAOB will make determinations whether the PRC authorities have allowed us to inspect and investigate completely or they have continued to obstruct.

The Holding Foreign Companies Accountable Act demands complete access. The agreement we signed with our Chinese counterparts guarantees complete access. And the PCAOB will accept nothing less than complete access when we make our determinations by the end of this year.

When I say no loopholes and no exceptions, I mean none.

Before we move on, I want to thank our dedicated teams of PCAOB professionals who have stepped up to do this important work.

Their sacrifices will help keep investors protected. And protecting investors is what this is all about.

Enforcement

From workers saving for retirement to parents saving to put their kids through college, and anyone who depends on the soundness of our capital

markets to invest and build for their future, protecting investors guides everything we do at the PCAOB.

And we have three critical tools to help us achieve that mission: standards, inspections, and enforcement.

Each of them serves a key function on its own. But they are strongest when they work together.

High standards set the foundation for high quality audits.

Quality inspections tell us where our standards could be improved, and they shine a light on audit deficiencies that can lead to investigations and enforcement actions.

Strong enforcement encourages compliance with our standards, and it informs where we should focus our inspections.

Together, all three help keep investors protected.

Last month, the Board released our draft strategic plan outlining goals to modernize our standards, enhance our inspections, and strengthen our enforcement.

Much of that work is already well underway.

For example, earlier this year, the Board announced one of the most ambitious standard-setting agendas in the PCAOB's history. Nine months into the first year of this new Board, we are already working to update more than 25 standards within eight standard-setting projects.

Our inspections team is constantly adjusting to be responsive to new and emerging risks across the globe – whether it's SPACs and de-SPAC transactions, cryptocurrencies, or how firms are addressing the effects of supply chain disruptions and rising costs on company operations.

Today, I'd like to focus on enforcement.

As our strategic plan makes clear, this Board is approaching enforcement with a renewed vigilance.

While we cannot talk about ongoing enforcement actions, I can assure you: we intend to use every tool in our enforcement toolbox and impose significant sanctions, where appropriate, to ensure there are consequences for putting investors at risk and that bad actors are removed. This includes substantial monetary penalties and significant or permanent individual bars and firm registration revocations.

We are looking at how we identify cases, the types of cases we pursue, and the sanctions we impose.

First, we are expanding our case identification process.

We are strengthening the process for our inspections team to refer potential violations they find for investigation and enforcement.

We are looking for patterns and conducting more sweeps. Sweeps enable us to get additional information from a number of firms at the same time on areas where we suspect that violations may be occurring. They make it harder for those violating our rules or standards to hide.

We are working closely with our fellow watchdog agencies to identify potential cases.

And we are encouraging the public to report potential violations. You can learn more about how to do so on the tips and referrals page at www.pcaobus.org.

Second, we are expanding the types of cases we are pursuing.

For any violation of PCAOB standards that is serious enough to put investors at risk, the excuse that "it only happened once" simply won't cut it. We will not hesitate to bring cases that hinge on only a single, serious wrongful act, whether reckless or negligent.

We aren't just pursuing individual wrongdoing – we're holding firms accountable in more situations, including for failing to appropriately staff or respond to the risks of an audit.

And we are going after cases where firms' quality controls aren't up to standard to keep investors protected.

Third, we're making sanctions count.

Under this Board, we've more than doubled our average penalties against individuals compared to the last five years. This includes the largest money penalty ever imposed on an individual in a settled case.

At the same time, we've increased our average penalties against firms by more than 65%.

In the past five years, the PCAOB assessed penalties against individuals less than half of the time and firms only about 86% of the time. This year it's 100%.

Just last week, we announced a settled disciplinary order permanently revoking a firm's registration and barring the firm's owner, as well as imposing a significant penalty, for interfering with the Board's inspection process.

It was the first settled action in PCAOB history with both a permanent revocation or bar and a significant penalty. And it demonstrates our commitment to remove bad actors from the profession and to deter misconduct.

Those who break the rules should know we won't be constrained by the types of cases the PCAOB has pursued in the past. We won't be limited to the level of penalties that have been seen before. And we will seek admissions of wrongdoing in appropriate cases – for example, where the conduct is intentional or egregious.

We mean business when it comes to enforcement because we can't afford not to.

As Senator Paul Sarbanes said shortly after he joined Republicans and Democrats to create the PCAOB 20 years ago: "If you don't protect the interests of the investors, it deals a major blow to the workings of the economic system. The U.S. capital markets have established a reputation for integrity because we have a system designed to screen out people who are trying to cut the corners and rig the system."

The PCAOB is proud to be part of that system Senator Sarbanes talked about because we know what's at stake.

At the beginning of this speech, I told you the PCAOB inspects and investigates in more than 50 countries. That is because companies around the world seek out U.S. capital markets as the gold standard.

But the integrity of our capital markets is not inevitable. It takes vigilance to guard against negligence, recklessness, and fraud that threatens our system and the people who depend on it.

At the PCAOB we are working hard to bring that vigilance to our standards, inspections, and enforcement every day.

You may visit: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-chair-williams-delivers-remarks-at-cii-fall-conference

PCAOB Chair Delivers Remarks at UCI Audit Committee Summit

Erica Y. Williams, at the ninth annual UCI Audit Committee Summit.

Thank you, Dr. [Patricia] Wellmeyer.

I will start by providing the standard disclaimer that the views that I express here are my own and not necessarily the views of my fellow Board Members or the PCAOB's staff.

I am delighted to be here and to have the chance to address this distinguished audience.

I'm also honored to be on an agenda with so many great speakers, starting with Commissioner Peirce.

Like all of you, I am really looking forward to Commissioner Peirce's remarks, which are always insightful and thought-provoking.

I am not the first PCAOB Board Member to address this summit. Since this event began in 2014, several Board Members have delivered keynote remarks here, because engaging with audit committees is vital to the work we do at the PCAOB.

In fact, since 2019, the PCAOB has held conversations with more than 1,000 audit committee chairs to hear your perspectives and insights on a broad range of topics.

After all, we share a common aim – audit committees are guided by a fiduciary responsibility, and the PCAOB is guided by our mission, but our goal is the same: to protect investors.

As Senator Paul Sarbanes said shortly after he helped create the PCAOB, "If you don't protect the interests of the investors, it deals a major blow to the workings of the economic system…Investors, after all, make the whole thing work."

This summer marked 20 years since Senator Sarbanes joined Representative Mike Oxley and Members from across both parties to create the PCAOB.

As we think about where we are going, it's worth reflecting on where we've been.

Lawmakers came together to pass the Sarbanes-Oxley Act nearly unanimously after major accounting scandals from Enron to WorldCom rocked our markets in the early 2000s.

Corporations were lying about their earnings and hiding their debt. And when it all came crashing down, investors lost billions, workers lost jobs and retirement savings, and trust in our markets was eroded.

Since then, the PCAOB has:

- Registered over 3,800 audit firms,

- Completed more than 4,300 firm inspections in 55 countries – reviewing more than 15,000 audits of public companies and over 1,000 broker-dealer engagements, and

- Issued more than 330 settled enforcement orders – and sanctioned more than 230 firms and 270 individuals.

And it has made a difference.

Multiple academic studies have found that PCAOB inspections improve audit quality, both here in the U.S. and in other countries where the PCAOB has inspection access.

We know that increasing audit quality boosts confidence in the credibility of financial reporting, which supports capital formation and is good for everyday investors.

Continuing to strengthen that credibility is a top priority for our Board as we carry out our mission to protect investors.

We understand that the integrity and success of our capital markets are not inevitable. Like the lawmakers who passed the Sarbanes-Oxley Act 20 years ago, we must continue to take action to keep investors protected today.

This summer, the Board released our five-year strategic plan, outlining four key goals:

- One, modernizing our standards,
- Two, enhancing our inspections,
- Three, strengthening our enforcement, and
- Four, improving organizational effectiveness.

To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-chair-williams-delivers-remarks-at-uci-audit-committee-summit

The Economic Outlook: Time to Let the Data Do the Talking

Governor Christopher J. Waller, Board of Governors of the Federal Reserve System, 17th Annual Vienna Macroeconomics Workshop, Vienna, Austria

Thank you, Klaus, and thank you for the invitation to speak at this workshop, which I have been attending since its very beginning in 2004.

Something that I love about this conference that has kept me coming back almost every year is its tradition of open inquiry and even some fun, on the one hand, combined with rigorous, critical analysis, on the other.

I am a supporter, and I guess a practitioner, of rigorous criticism, because, as you may have heard, the conference award given each year for "outstanding critic" was named for me.

Based on the standard I set, the person who wins the award is also known as the "most annoying participant." I suppose it was only karma that a guy like me who likes to dish out the criticism would end up in a job that receives plenty of it.

Kidding aside, I do consider being the namesake for this award a great honor, and just to make sure I don't get too much of a swelled head, by tradition the conference organizers purposefully misspell my name.

My subject today is the outlook for the U.S. economy and the Federal Reserve's ongoing campaign to bring down inflation and achieve our 2 percent objective.

There are three takeaways from my speech today. First, inflation is far too high, and it is too soon to say whether inflation is moving meaningfully and persistently downward.

The Federal Open Market Committee (FOMC) is committed to undertake actions to bring inflation back down to our 2 percent target. This is a fight we cannot, and will not, walk away from.

The second takeaway is that the fears of a recession starting in the first half of this year have faded away and the robust U.S. labor market is giving us the flexibility to be aggressive in our fight against inflation.

For that reason, I support continued increases in the FOMC's policy rate and, based on what I know today, I support a significant increase at our next meeting on September 20 and 21 to get the policy rate to a setting that is clearly restricting demand.

The final takeaway is that I believe forward guidance is becoming less useful at this stage of the tightening cycle.

Future decisions on the size of additional rate increases and the destination for the policy rate in this cycle should be solely determined by the incoming data and their implications for economic activity, employment, and inflation.

Based on all of the data that we have received since the FOMC's last meeting, I believe the policy decision at our next meeting will be straightforward.

Because of the strong labor market, right now there is no tradeoff between the Fed's employment and inflation objectives, so we will continue to aggressively fight inflation.

Inflation is widespread, driven by strong demand that has only begun to moderate, by an ongoing lag in labor force participation, and by supply chain problems that may be improving in some areas but are still considerable.

For these reasons, I expect it will take some time before inflation moves back to our 2 percent goal, and that the FOMC will be tightening policy into 2023. But the answers to questions of "how high?" and "for how long?" will depend solely on incoming data.

Since I last spoke in July, I think the argument that we entered a recession in the first half of 2022 has pretty much ended—we didn't. With each passing week, the absence of any indication of a recession in spending or employment data buries that recession argument a little deeper.

We understand some of the factors that lowered the gross domestic product (GDP) numbers in the first half, and a debate continues about other possible factors, such as mismeasurement, potentially underreporting GDP.

What we can say is that after the Fed telegraphed its policy pivot to tightening in the latter months of 2021 and began raising rates in the first quarter of this year, demand and economic activity slowed in the first half of 2022 from the strong pace of 2021.

Data suggest an uptick in consumption growth in the third quarter. Meanwhile, the Atlanta Fed's GDPNow model forecasts real GDP will grow 2.6 percent this quarter, though other estimates are a touch below this prediction.

Spending data are supportive of continued expansion. Nominal retail sales overall were flat in July, but that is mainly because falling gasoline and auto prices—which is good news—held back sales in those sectors.

Excluding that, retail sales rose 0.7 percent, suggesting that discretionary spending grew solidly. Businesses also continued to expand production and spending. Total industrial production increased 0.6 percent in July, standing 3.9 percent above its level a year ago.

Forward-looking indicators of manufacturing activity, such as new orders indexes in various manufacturing surveys, are softer than earlier in the year, but most (and in particular the positive August reading from the ISM) are not suggestive of a material pullback in manufacturing activity.

Meanwhile, the non- manufacturing ISM report suggests continuing growth, with its new orders index rising to a solid level last month.

But there are signs of moderation in economic activity, which is what the FOMC is trying to achieve by tightening monetary policy. Not surprisingly, higher interest rates this year are slowing activity in the housing market.

There have been declines in construction of single-family homes for a number of months, with permits and home starts both decreasing in July.

Sales of existing and new single-family homes have also slowed. Existing home sales fell by 5.9 percent to a seasonally adjusted annual rate of 4.8 million homes in July.

While the imbalance between housing supply and demand remains significant, it has meaningfully improved. The inventory of unsold new and existing homes has more than doubled since January.

While the three months supply of existing home is still below levels before the pandemic, the eleven months of new home inventory is the highest since the spring of 2009.

This latter statistic has raised concerns by some about a significant downturn looming in the housing market, but an important caveat is that much of the current elevated inventory reflects the recent low rate of housing completion due to continued supply constraints.

Many of these new homes for sale are still under construction, and as supply constraints ease, builders will be able deliver more completed homes to a market where the supply of existing homes remains tight. All that said, the housing market is a significant channel for monetary policy, and I will be watching this sector carefully.

The FOMC's goal is that the tightening in monetary policy slows aggregate demand so that it is in better alignment with supply across all sectors of the economy.

My expectation is that strong household savings, the tight labor market, and additional availability of manufactured goods as supply chains constraints continue to resolve will allow households to make long-awaited purchases, which will provide a partial offset to tighter policy. That will support a slowing, rather than a contraction, in demand.

Turning to the very strong labor market, private payroll employment has been increasing at an average of nearly 400,000 a month over the last several months.

Unemployment rose two tenths of a percent in August to 3.7 percent, in part reflecting an increase in the labor force participation rate, but still stands at a very low level.

The increase in participation was welcome news, but this rate is still far below that achieved before the pandemic, when unemployment was roughly as low as today.

We are facing worker shortages in many sectors of the economy. Job openings have started to decline a bit but remain very elevated. These data confirm that the Fed is hitting its full employment mandate, so all my attention is on bringing inflation down.

Inflation slowed in July, which was a very encouraging development. Headline inflation for both the consumer price index and the index derived from personal consumption expenditures (PCE)—the Fed's preferred measure—slowed, largely due to continuing declines in prices for gasoline and other petroleum products.

Excluding volatile energy and food prices, core inflation for these two indexes also stepped down from the rapid increases of earlier this year, but it is still too early to say that inflation is moving meaningfully and persistently downward.

Inflation is still widespread. For both headline and core inflation, at least 60 percent of the underlying categories of different goods and services increased by 3 percent or more.

Prices for housing services are elevated and still rising. Core goods inflation continues to run well above its pre-pandemic level.

Inflation for services excluding housing has moved up this past year in part due to consumers shifting back to more normal activities outside the household as social distancing has eased.

Looking ahead, I will be focusing on a number of factors that will influence inflation. On housing services—rent and the so-called owners' equivalent rent —I expect to see sizable increases in this component of inflation for a while as the recent rise in new rentals makes its way into aggregate price measures.

In a speech in March, I noted that, based on various measures of asking rents, some analysts were predicting that the rate of rent inflation in the consumer price index could double in 2022, and so far it is on pace to more than double.

Owners-equivalent rent is similarly on pace to nearly double this year. Sometime early next year, though, I expect to see the upward pressure on inflation from these forces to ease as future increases in new or renewed leases moderate and the full effects of monetary policy tightening make their way to housing services prices.

Beyond housing, I expect goods price inflation to continue to moderate as monetary policy now and going forward slows the pace of increase in aggregate demand, supply problems ease, and supply and demand come into better balance.

There is some evidence that goods supply production and delivery problems tied to the pandemic are improving, with supplier delivery times and reports of items in short supply continuing to drop.

In terms of service price inflation, we saw a step-down in airfares and other travel-related services last month, but I am uncertain about how these services, as well as food services, and nonmarket services prices will evolve going forward.

Nominal wages have been growing quickly, and I'll be watching closely to see how wage growth evolves and feeds into inflation.

The Atlanta Fed's Wage Growth Tracker hit another record in July for its 24 years of data, a 12-month rate of 6.7 percent wage growth.

I don't expect wage increases to ease up much unless and until there is a significant softening in the labor market.

One way to anticipate future wage growth is through quit rates. Most people who quit their jobs are moving to others that pay significantly better, so I take quits as one signal about where wages are headed in the near term.

Quits are near their highest level over the 22 years that the government has tracked them, but they have come down from the start of this year, and further decreases would bring them closer to the level they were at immediately before the pandemic, when wages were growing much more slowly than today.

Another factor that I will be watching closely is longer-term inflation expectations, which I believe significantly influence inflation.

As inflation moved higher over the past year and a half, measures of short-term inflation expectations moved up notably, but measures of longer-term expectations rose only a little and generally stand near levels seen in the years before the pandemic, when inflation was low.

In fact, several measures of longer-term expectations have edged lower over the past couple of months. To me, this means that the public retains confidence that the Fed will be able to rein in inflation in the medium term.

To sum up, while I welcome promising news about inflation, I don't yet see convincing evidence that it is moving meaningfully and persistently down along a trajectory to reach our 2 percent target.

I keep in mind that a year ago we saw similarly promising evidence of inflation moderating for several months before it jumped up to a high and then very high level.

Those earlier inflation readings probably delayed our pivot to tightening monetary policy by a few months.

The consequences of being fooled by a temporary softening in inflation could be even greater now if another misjudgment damages the Fed's credibility.

So, until I see a meaningful and persistent moderation of the rise in core prices, I will support taking significant further steps to tighten monetary policy.

Now let me lay out the implications of this outlook for monetary policy. Since March, the FOMC has raised our policy target range from near zero to between 2-1/4 and 2-1/2 percent.

That puts the upper bound of the current target range at the median of FOMC participants' longer-run projection for the policy rate, as recorded in the June Summary of Economic Projections (SEP).

This long-run rate is effectively where participants think the policy rate would settle when the economy is growing at its potential and inflation is at our 2 percent target.

This is a good definition of success when employment and inflation are near our goals and no help is needed from monetary policy. But that isn't the case now; inflation is far from our goal, so more action is needed.

The policy rate will have to move meaningfully above this neutral level to further restrain aggregate demand and put more downward pressure on prices.

Looking ahead to our next meeting, I support another significant increase in the policy rate. But, looking further out, I can't tell you about the appropriate path of policy. The peak range and how fast we will move there will depend on data we will receive about the economy.

Earlier this year, when we were ending asset purchases, inflation was quite elevated, and we were lifting the target range off the effective lower bound, so it made sense to provide forward guidance to help convey the urgency the FOMC felt about tightening monetary policy.

Forward guidance was useful in helping the public understand how quickly we expected to tighten, and we saw longer-term interest rates move up quite rapidly as a result of these communications. And additional hikes should lead to further restraint in aggregate demand.

As we continue to raise rates, we need to see, month by month, how households and businesses are adjusting to the tighter financial conditions, and how that adjustment is affecting inflation. We shouldn't be estimating what the peak level of the target range will be and how quickly we will get there, because those details are much more dependent on what new economic data tell us than was the case when the only direction for the federal funds rate to go was up—and up by a lot.

This is not to suggest that I anticipate rate increases stopping very soon. I expect that getting inflation to fall meaningfully and persistently toward our 2 percent target will require increases in the target range for the federal funds rate until at least early next year.

But don't ask me about the policy path because I truly don't know—it will depend on the data.

Six months ago, I would not have thought that we would be where we are today, with inflation so far from our target, after significantly tightening policy with a series of large rate increases and by shrinking the balance sheet.

There are a range of possibilities for how the economy will perform, however, and we can talk about the implications of that range. Say, for example, that inflation follows the path laid out in the June SEP, which has core PCE inflation falling to 4.3 percent in the fourth quarter of 2022 and then moving toward 2 percent over 2023 and 2024. In that case, I would support our policy rate peaking near 4 percent.

But based on the experience of the past year and half, it would be foolish to express great confidence that this plausible path will come to pass. Instead, it is important to consider the range of possibilities and the appropriate policy responses.

For example, if inflation does not moderate or rises further this year, then, in my view, the policy rate will probably need to move well above 4 percent. Alternatively, if inflation suddenly decelerates, then, in my view, the policy rate might peak at less than 4 percent.

One thing that is more predictable and has a significant effect on tightening policy over time is the shrinking of the Fed's holdings of assets as maturing securities run off our balance sheet. Starting this month, the Fed is shedding $60 billion a month in Treasury securities and up to $35 billion a month in agency mortgage-backed securities.

This action effectively increases the supply of securities in the hands of private investors and will thus put upward pressure on interest rates, as private investors must now be enticed to hold these assets.
All told, the FOMC has taken unprecedented and decisive policy actions this year to quickly increase the policy rate in response to high inflation. But where we stand now is not good enough. Though the labor market is strong, inflation is too elevated.

So I support another significant hike in two weeks. After that, the tightening path will continue until we see clear and convincing evidence that inflation is moving meaningfully and persistently down to our 2 percent target.

The pace of tightening is uncertain; it will depend on the data. No matter what, I am ready and willing to do what it takes to bring inflation down.

To read more:
https://www.federalreserve.gov/newsevents/speech/waller20220909a.htm

MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone

Microsoft Threat Intelligence Center (MSTIC), Microsoft Detection and Response Team (DART), Microsoft 365 Defender Research Team

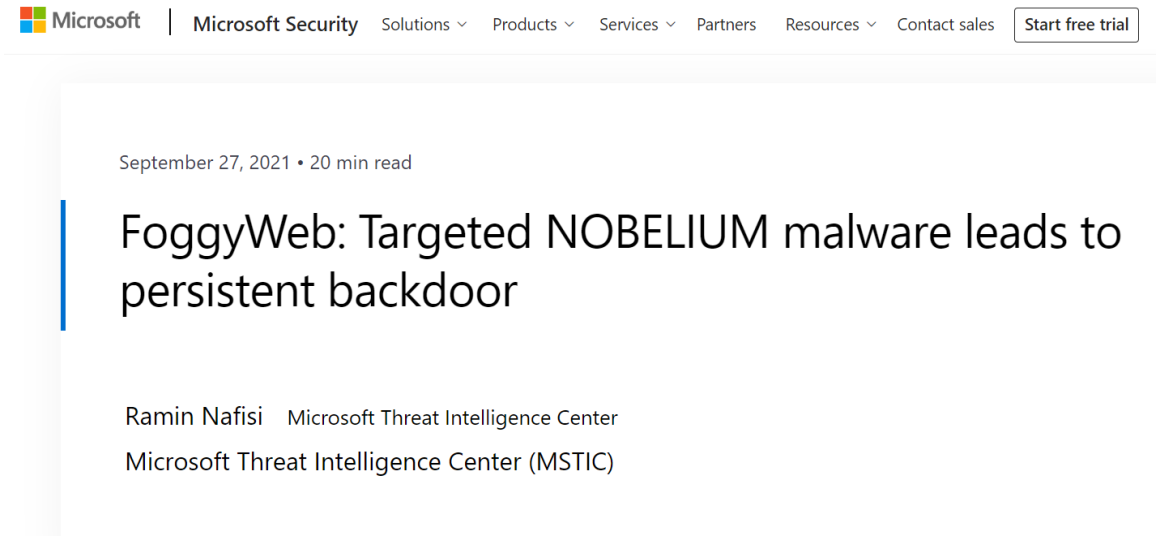
Microsoft

Microsoft security researchers have discovered a post-compromise capability we're calling MagicWeb, which is used by a threat actor we track as NOBELIUM to maintain persistent access to compromised environments.

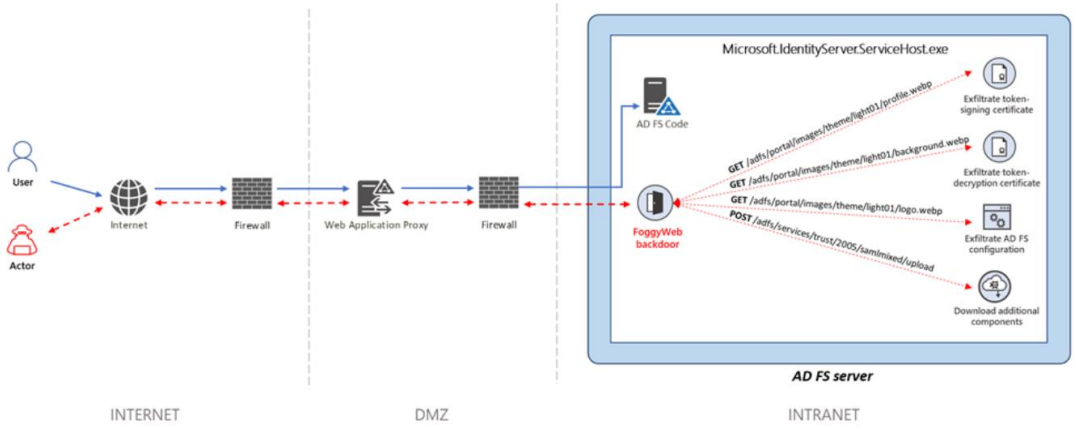
NOBELIUM remains highly active, executing multiple campaigns in parallel targeting government organizations, non-governmental organizations (NGOs), intergovernmental organizations (IGOs), and think tanks across the US, Europe, and Central Asia.

The Microsoft Threat Intelligence Center (MSTIC) assesses that MagicWeb was likely deployed during an ongoing compromise and was leveraged by NOBELIUM possibly to maintain access during strategic remediation steps that could preempt eviction.

NOBELIUM has used abuse of identities and credentialed access as a method for maintaining persistence, and a specialized capability like MagicWeb is not novel for the actor: in September 2021, Microsoft disclosed a post-exploitation capability named FoggyWeb with methods and intent similar to MagicWeb. You may visit: https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/



The diagram below illustrates the methodology used by the actor to communicate with the FoggyWeb backdoor located on a compromised internet-facing AD FS server.



FoggyWeb was capable of exfiltrating the configuration database of compromised AD FS servers, decrypting token-signing certificates and token-decryption certificates, and downloading and executing additional malware components.

MagicWeb goes beyond the collection capabilities of FoggyWeb by facilitating covert access directly.

MagicWeb is a malicious DLL that allows manipulation of the claims passed in tokens generated by an Active Directory Federated Services (AD FS) server.

It manipulates the user authentication certificates used for authentication, not the signing certificates used in attacks like Golden SAML.

NOBELIUM was able to deploy MagicWeb by first gaining access to highly privileged credentials and moving laterally to gain administrative privileges to an AD FS system. This is not a supply chain attack.

The attacker had admin access to the AD FS system and replaced a legitimate DLL with their own malicious DLL, causing malware to be loaded by AD FS instead of the legitimate binary.

The backdoor was discovered by Microsoft's Detection and Response Team (DART) in coordination with MSTIC and Microsoft 365 Defender Research during an ongoing incident response investigation.

Microsoft is sharing this information with consent from the client. At the time of this investigation, MagicWeb appears to be highly targeted.
Like domain controllers, AD FS servers can authenticate users and should therefore be treated with the same high level of security.

Customers can defend against MagicWeb and other backdoors by implementing a holistic security strategy including the AD FS hardening guidance. In the case of this specific discovery, MagicWeb is one step of a much larger intrusion chain that presents unique detection and prevention scenarios.

With all critical infrastructure such as AD FS, it is important to ensure attackers do not gain administrative access.

Once attackers gain administrative access, they have many options for further system compromise, activity obfuscation, and persistence.

We recommend that any such infrastructure is isolated, accessible only by dedicated admin accounts, and regularly monitored for any changes.

Other security measures that can prevent this and other attacks include credential hygiene to prevent lateral movement. AD FS is an on-premises server, and as with all on-premises servers, deployments can get out of date and/or go unpatched, and they can be impacted by local environment compromises and lateral movement.

For these reasons, migration to a cloud-based identity solution such as Azure Active Directory for federated authentication is recommended for the robust security it provides.

See the mitigation section below for more information.

Though we assess the capability to be in limited use, Microsoft anticipates that other actors could adopt similar methodologies and therefore recommends customers review hardening and mitigation guidance provided in this blog.

How MagicWeb subverts authentication

MagicWeb is a post-compromise malware that can only be deployed by a threat actor after gaining highly privileged access to an environment and moving laterally to an AD FS server.

To achieve their goal of maintaining persistent access to an environment by validating authentication for any user account on the AD FS server, NOBELIUM created a backdoored DLL by copying the legitimate Microsoft.IdentityServer.Diagnostics.dll file used in AD FS operations. The legitimate version of this file is catalog signed by Microsoft and is normally loaded by the AD FS server at startup to provide debugging capabilities. NOBELIUM's backdoored version of the file is unsigned.

The threat actor's highly privileged access that allowed them to access the AD FS server meant they could have performed any number of actions in the environment, but they specifically chose to target an AD FS server to facilitate their goals of persistence and information theft during their operations.

After gaining administrative access to an AD FS server via elevation of privilege and lateral movement, the loading of NOBELIUM's malicious Microsoft.IdentityServer.

To read more:
https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/

Chief Information Officers, Private Sector Practices Can Inform Government Roles

United States Government Accountability Office
Report to Congressional Committees

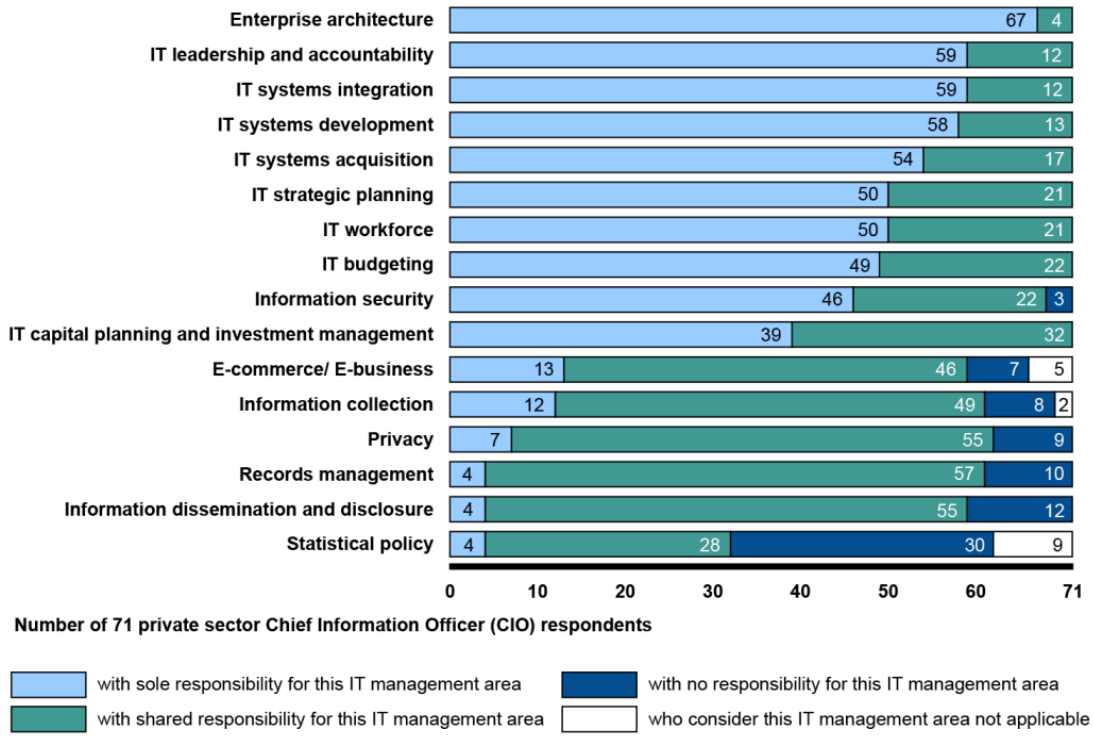
What GAO Found

A majority of the 71 private sector Chief Information Officer (CIO) survey respondents reported having responsibilities that aligned with those of agency CIOs in 13 of 14 key IT management areas.

These areas include strategic planning, investment management, and information security. One area of responsibility (the statistical policy area) was reported by more than half of respondents as being outside their scope of responsibility.

In addition, CIO respondents also reported sharing responsibility with other executives in each IT management area (see figure 1).

Figure 1: Extent of Sharing of IT Management Area Responsibilities Reported by 71 Private Sector Chief Information Officer (CIO) Respondents



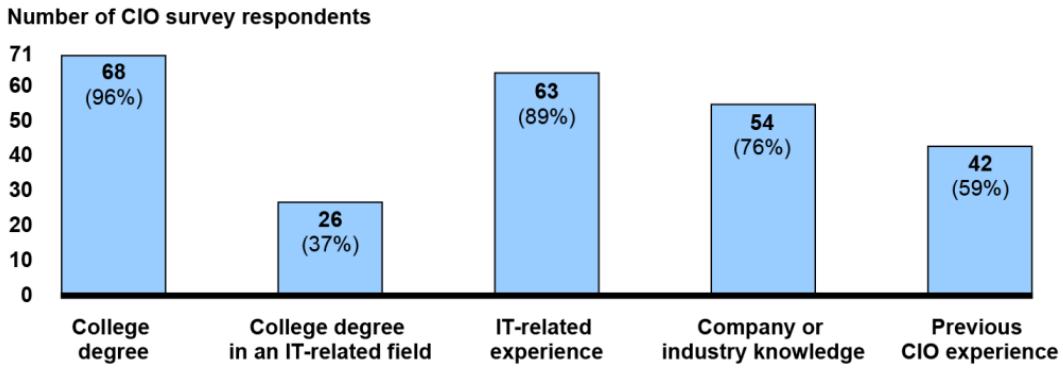
Source: GAO analysis of data from 71 private sector CIO survey respondents. | GAO-22-104603

Private sector CIO respondents were highly educated and experienced, with a majority reporting previous IT-related experience, previous CIO experience, industry knowledge, and a college degree (see figure 2).

Notably, a majority of respondents reported that their degrees were not IT-related. Respondents reported an average tenure in their current CIO role of about 6 years.

Among respondents, CIOs with more authority over technology-related decisions tended to have a higher level of previous CIO experience, as well as the longest tenures.

Figure 2: Qualifications and Experience of Private Sector Chief Information Officer (CIO) Respondents



Source: GAO analysis of data from 71 private sector CIO survey respondents. | GAO-22-104603

This graph shows selected responses from two survey questions. The variables are categorical and the numbers are not intended to add to 71 or the percentages to 100 percent.

Responsibilities currently assigned to the Federal CIO correspond to those of agency CIOs in 10 of the 14 key IT management areas.
The Federal CIO's responsibilities also correspond to those of private sector survey respondents in each of five responsibility areas directly relevant to the roles of both.

However, the Federal CIO position is not established in law, and its main legal authorities remain those established in 2002 for the OMB position from which the role was established.

As such, its responsibilities are often more limited in key CIO management areas than those of the other types of CIOs.

For example, the Federal CIO is not responsible for ensuring that cybersecurity duties are carried out. By formalizing the Federal CIO position and establishing responsibilities and authorities over government-wide IT management, the position's impact over federal IT may be more consistent over time and across administrations.

Private sector and former agency CIOs participating in panel discussions reported challenges faced by federal agency CIOs.

Specifically, private sector CIO panelists stated that collaboration between the CIO and other senior executives is essential to driving successful business outcomes.

Conversely, former federal CIO panelists reported difficulty achieving meaningful collaboration with other managers. In addition, private sector panelists stated that their companies often look for managerial skills, such as project management skills, when hiring CIOs.

By contrast, former agency CIO panelists stated that technical skills are often a primary driver in the selection of agency CIOs.

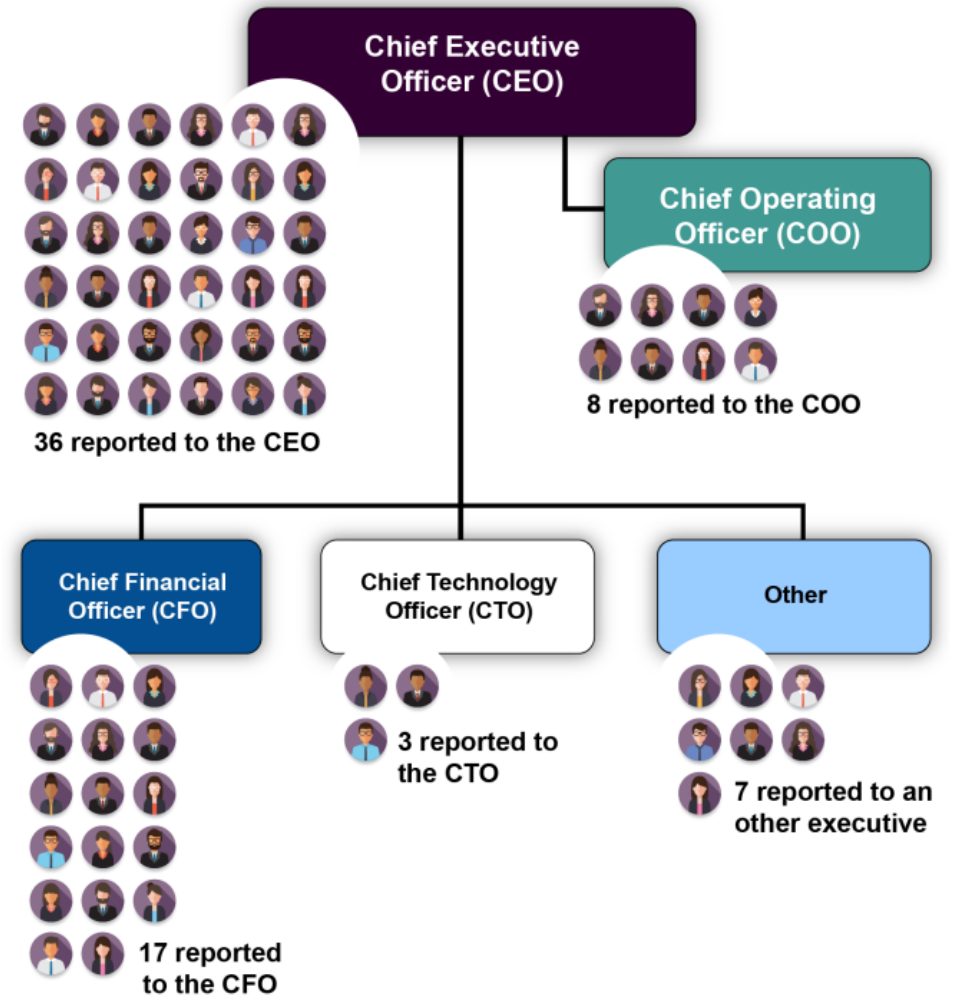
Fostering shared collaboration and increasing focus on managerial skillsets for agency CIOs could assist federal agencies and their CIOs in securing resources and implementing IT priorities.

The Level of IT Responsibilities Shared by Private Sector CIO Respondents Varied Based on Their Reporting Structure

Private sector CIOs who responded to our survey had direct reporting relationships to several different senior executives at their companies.

For example, approximately half of private sector CIOs reported directly to their company's CEO, and about a quarter to their company's CFO. The remainder of the CIO respondents reported directly to other executives, such as their COO, chief technology officer (CTO), president, chief administrative officer, chief growth officer, or the chief of corporate operations. Figure 3 shows the percent of CIO respondents directly reporting to each of the four primary types of senior executives mentioned by CIOs, as well as those reporting to executives other than those four.

Figure 3: Reporting Structure for 71 Private Sector Chief Information Officer (CIO) Respondents



Source: GAO analysis of data from 71 private sector CIO survey respondents; images: sapannpix/stock.adobe.com. | GAO-22-104603

To read more:
https://www.gao.gov/assets/gao-22-104603.pdf

Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement

Good afternoon. Thank you, Dean McKenzie, for the introduction and for hosting us today. I'm happy to be back at NYU, and to see so many friends and former colleagues in the room.

Let me start by acknowledging some of my DOJ colleagues who are here. That includes the U.S. Attorneys for the Southern and Eastern Districts of New York, New Jersey, and Connecticut.

But just as importantly, we're joined in person and on the livestream by line prosecutors, agents, and investigative analysts—the career men and women who do the hard work, day in and day out, to make great cases and hold wrongdoers accountable.

I also want to recognize our federal and state partners who play a critical role in corporate enforcement. And of course, let me also thank Professor Arlen and the NYU Program on Corporate Compliance and Enforcement for arranging this event and for serving as a bridge between the worlds of policymaking and academia.

Addressing corporate crime is not a new subject for the Justice Department. In the aftermath of Watergate, Attorney General Edward Levi was tasked not only with restoring the Department's institutional credibility, but also with rebuilding its corporate enforcement program.

In a 1975 speech, he told prosecutors that there was great demand to be more aggressive against, what he called, "white collared crime." He explained his distaste for that term, saying that it suggested a distinction in law enforcement based upon social class. But, nonetheless, he acknowledged that it was an area that needed to be given "greater emphasis." These words are as true today as they were then.

But Attorney General Levi also said that efforts to fight corporate crime were hampered by a lack of resources, specially trained investigators, and other issues. He answered those complaints as all great Attorneys General do—he said his Deputy Attorney General would take care of it. For at least a half-century, therefore, it has been the responsibility of my predecessors to set corporate criminal policy for the Department, and I follow in their footsteps.

Last October, I announced immediate steps the Justice Department would take to tackle corporate crime.

I also formed the Corporate Crime Advisory Group, a group of DOJ experts tasked with a top-to-bottom review of our corporate enforcement efforts.

To get a wide range of perspectives, we met with a broad group of outside experts, including public interest groups, ethicists, academics, audit committee members, in-house attorneys, former corporate monitors, and members of the business community and defense bar. Many of these people are here today.

Our meetings sparked discussions on individual accountability and corporate responsibility; on predictability and transparency; and on the ways enforcement policies must square with the realities of the modern economy. Every meeting resulted in some idea or insight that was helpful and that we sought to incorporate into our work. Today, you will hear how these new policies reflect this diverse input.

Let me turn now to substance—and the changes the Department is implementing to further strengthen how we prioritize and prosecute corporate crime.

First, I'll reiterate that the Department's number one priority is individual accountability—something the Attorney General and I have made clear since we came back into government. Whether wrongdoers are on the trading floor or in the C-suite, we will hold those who break the law accountable, regardless of their position, status, or seniority.

Second, I'll discuss our approach to companies with a history of misconduct. I previously announced that prosecutors must consider the full range of a company's prior misconduct when determining the appropriate resolution. Today, I will outline additional guidance for evaluating corporate recidivism.

Third, I'll highlight new Department policy on voluntary self-disclosures, including the concrete and positive consequences that will flow from self-disclosure. We expect good companies to step up and own up to misconduct. Voluntary self-disclosure is an indicator of a working compliance program and a healthy corporate culture. Those companies who own up will be appropriately rewarded in the Department's approach to corporate crime.

Fourth, I'll detail when compliance monitors are appropriate and how we can select them equitably and transparently. Today, I am also directing Department prosecutors to monitor those monitors: to ensure they remain on the job, on task, and on budget.

Finally, I'll discuss how the Department will encourage companies to shape financial compensation around promoting compliance and avoiding

improperly risky behavior. These steps include rewarding companies that claw back compensation from employees, managers, and executives when misconduct happens. No one should have a financial interest to look the other way or ignore red flags. Corporate wrongdoers—rather than shareholders—should bear the consequences of misconduct.

Taken together, the policies we're announcing today make clear that we won't accept business as usual. With a combination of carrots and sticks—with a mix of incentives and deterrence—we're giving general counsels and chief compliance officers the tools they need to make a business case for responsible corporate behavior. In short, we're empowering companies to do the right thing—and empowering our prosecutors to hold accountable those that don't.

Individual Accountability

Let me start with our top priority for corporate criminal enforcement: going after individuals who commit and profit from corporate crime.

In the last year, the Department of Justice has secured notable trial victories, including convictions of the founder and chief operating officer of Theranos; convictions of J.P. Morgan traders for commodities manipulation; the conviction of a managing director at Goldman Sachs for bribery; and the first-ever conviction of a pharmaceutical CEO for unlawful distribution of controlled substances.

Despite those steps forward, we cannot ignore the data showing overall decline in corporate criminal prosecutions over the last decade. We need to do more and move faster. So, starting today, we will take steps to empower our prosecutors, to clear impediments in their way, and to expedite our investigations of individuals.

To do that, we will require cooperating companies to come forward with important evidence more quickly.

Sometimes we see companies and counsel elect—for strategic reasons—to delay the disclosure of critical documents or information while they consider how to mitigate the damage or investigate on their own. Delayed disclosure undermines efforts to hold individuals accountable. It limits the Department's ability to proactively pursue leads and preserve evidence before it disappears. As time goes on, the lapse of statutes of limitations, dissipation of evidence, and the fading of memories can all undermine a successful prosecution.

In individual prosecutions, speed is of the essence.

Going forward, undue or intentional delay in producing information or documents—particularly those that show individual culpability—will result in the reduction or denial of cooperation credit. Gamesmanship with disclosures and productions will not be tolerated.

If a cooperating company discovers hot documents or evidence, its first reaction should be to notify the prosecutors. This requirement is in addition to prior guidance that corporations must provide all relevant, non-privileged facts about individual misconduct to receive any cooperation credit.

Separately, Department prosecutors will work to complete investigations and seek warranted criminal charges against individuals prior to or at the same time as entering a resolution against a corporation. Sometimes the back-and-forth of resolving with a company can bog down individual prosecutions, since our prosecutors have finite resources.

In cases where it makes sense to resolve a corporate case first, there must be a full investigative plan outlining the remaining work to do on the individual cases and a timeline for completing that work.

Collectively, this new guidance should push prosecutors and corporate counsel alike to feel they are "on the clock" to expedite investigations, particularly as to culpable individuals. While many companies and prosecutors follow these principles now, this guidance sets new expectations about the sequencing of investigations and clarifies the Department's priorities.

History of Misconduct

Now, it's safe to say that no issue garnered more commentary in our discussions than the commitment we made last year to consider the full criminal, civil, and regulatory record of any company when deciding the appropriate resolution.

That decision was driven by the fact that between 10% and 20% of large corporate criminal resolutions have involved repeat offenders.

We received many recommendations about how to contextualize historical misconduct, to develop a full and fair picture of the misconduct and corporate culture under review. We heard about the need to evaluate the regulatory environment that companies operate in, as well as the need to consider the age of the misconduct and subsequent reforms to the company's compliance culture.

In response to that feedback, today, we are releasing additional guidance about how such histories will be evaluated. Now let me emphasize a few points.

First, not all instances of prior misconduct are created equal. For these purposes, the most significant types of prior misconduct will be criminal resolutions here in the United States, as well as prior wrongdoing involving the same personnel or management as the current misconduct. But past actions may not always reflect a company's current culture and commitment to compliance. So, dated conduct will generally be accorded less weight.

And what do we mean by dated? Criminal resolutions that occurred more than 10 years before the conduct currently under investigation, and civil or regulatory resolutions that took place more than five years before the current conduct.

We will also consider the nature and circumstances of the prior misconduct, including whether it shared the same root causes as the present misconduct. Some facts might indicate broader weaknesses in the compliance culture or practices, such as wrongdoing that occurred under the same management team or executive leadership. Other facts might provide important mitigating context.

For example, if a corporation operates in a highly regulated industry, its history should be compared to others similarly situated, to determine if the company is an outlier.

Separately, we do not want to discourage acquisitions that result in reformed and improved compliance structures. We will not treat as recidivists companies with a proven track record of compliance that acquire companies with a history of compliance problems, so long as those problems are promptly and properly addressed post-acquisition.

Finally, I want to be clear that this Department will disfavor multiple, successive non-prosecution or deferred prosecution agreements with the same company. Before a prosecution team extends an offer for a successive NPA or DPA, Department leadership will scrutinize the proposal. That will ensure greater consistency across the Department and a more holistic approach to corporate recidivism.

Companies cannot assume that they are entitled to an NPA or a DPA, particularly when they are frequent flyers. We will not shy away from bringing charges or requiring guilty pleas where facts and circumstances require. If any corporation still thinks criminal resolutions can be priced in as the cost of doing business, we have a message—times have changed.

Voluntary Self-Disclosure

That said, the clearest path for a company to avoid a guilty plea or an indictment is voluntary self-disclosure. The Department is committed to providing incentives to companies that voluntarily self-disclose misconduct to the government. In many cases, voluntary self-disclosure is a sign that the company has developed a compliance program and has fostered a culture to detect misconduct and bring it forward.

Our goal is simple: to reward those companies whose historical investments in compliance enable voluntary self-disclosure and to incentivize other companies to make the same investments going forward.

Voluntary self-disclosure programs, in various Department components, have already been successful. Take, for example, the Antitrust Division's Leniency Program, the Criminal Division's voluntary disclosure program for FCPA violations, and the National Security Division's program for export control and sanctions violations. We now want to expand those policies Department-wide.

We also want to clarify the benefits of promptly coming forward to self-report, so that chief compliance officers, general counsels, and others can make the case in the boardroom that voluntary self-disclosure is a good business decision.

So, for the first time ever, every Department component that prosecutes corporate crime will have a program that incentivizes voluntary self-disclosure. If a component currently lacks a formal, documented policy, it must draft one.

Predictability is critical. These policies must provide clear expectations of what self-disclosure entails. And they must identify the concrete benefits that a self-disclosing company can expect.

I am also announcing common principles that will apply across these voluntary self-disclosure policies. Absent aggravating factors, the Department will not seek a guilty plea when a company has voluntarily self-disclosed, cooperated, and remediated misconduct. In addition, the Department will not require an independent compliance monitor for such a corporation if, at the time of resolution, it also has implemented and tested an effective compliance program.

Simply put, the math is easy: voluntary self-disclosure can save a company hundreds of millions of dollars in fines, penalties, and costs. It can avoid reputational harms that arise from pleading guilty. And it can reduce the risk of collateral consequences like suspension and debarment in relevant industries.

If you look at recent cases, you can see the value proposition. Voluntary self-disclosure cases have resulted in declinations and non-prosecution agreements with no significant criminal penalties. By contrast, recent cases that did not involve self-disclosure have resulted in guilty pleas and billions of dollars in criminal penalties, this year alone. I expect that resolutions over the next few months will reaffirm how much better companies fare when they come forward and self-disclose.

Independent Compliance Monitors

Let me turn to monitors. Over the past year of discussions, we heard a call for more transparency to reduce suspicion and confusion about monitors. Today, we're addressing those concerns.

First, we are releasing new guidance for prosecutors about how to identify the need for a monitor, how to select a monitor, and how to oversee the monitor's work to increase the likelihood of success.

Second, going forward, all monitor selections will be made pursuant to a documented selection process that operates transparently and consistently.

Finally, Department prosecutors will ensure that the scope of every monitorship is tailored to the misconduct and related compliance deficiencies of the resolving company. They will receive regular updates to verify that the monitor stays on task and on budget. We at the Department of Justice are not regulators, nor do we aspire to be. But where we impose a monitor, we recognize our obligations to stay involved and monitor the monitor.

Corporate Culture

As everyone here knows, it all comes back to corporate culture. Having served as both outside counsel and a board member in the past, I know the difficult decisions and trade-offs companies face about how to invest corporate resources, structure compliance programs, and foster the right corporate culture.

In our discussions leading to this announcement, we identified encouraging trends and new ways in which compliance departments are being strengthened and sharpened. But resourcing a compliance department is not enough; it must also be backed by, and integrated into, a corporate culture that rejects wrongdoing for the sake of profit. And companies can foster that culture through their leadership and the choices they make.

To promote that culture, an increasing number of companies are choosing to reflect corporate values in their compensation systems.

On the deterrence side, those companies employ clawback provisions, the escrowing of compensation, and other ways to hold financially accountable individuals who contribute to criminal misconduct. Compensation systems that clearly and effectively impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance.

On the incentive side, companies are building compensation systems that use affirmative metrics and benchmarks to reward compliance-promoting behavior.

Going forward, when prosecutors evaluate the strength of a company's compliance program, they will consider whether its compensation systems reward compliance and impose financial sanctions on employees, executives, or directors whose direct or supervisory actions or omissions contributed to criminal conduct. They will evaluate what companies say and what they do, including whether, after learning of misconduct, a company actually claws back compensation or otherwise imposes financial penalties.

I have asked the Criminal Division to develop further guidance by the end of the year on how to reward corporations that employ clawback or similar arrangements. This will include how to help shift the burden of corporate financial penalties away from shareholders—who frequently play no role in misconduct—onto those more directly responsible.

Conclusion

But we're not done.

We will continue to engage and protect victims—workers, consumers, investors, and others.
We will continue to find ways to improve our approach to corporate crime, such as by enhancing the effectiveness of the federal government's system for debarment and suspension.

We will continue to seek targeted resources for corporate criminal enforcement, including the $250 million we are requesting from Congress for corporate crime initiatives next year.

Today's announcements are fundamentally about individual accountability and corporate responsibility. But they are also about ownership and choice.

Companies should feel empowered to do the right thing—to invest in compliance and culture, and to step up and own up when misconduct occurs. Companies that do so will welcome the announcements today. For those who don't, however, our department prosecutors will be empowered, too—to hold accountable those who don't follow the law.

Thank you again for having me here today. I look forward to taking some questions.

To read more: https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement

Request for Information and Comment

The Application and Use of the PCAOB's Interim Attestation Standards

The staff of the Public Company Accounting Oversight Board is requesting information and public comment on matters related to the application and use of the Board's interim attestation standards.

In April 2003, the Board adopted on an interim basis certain attestation standards from the American Institute of Certified Public Accountants. These standards have continued in effect substantially as they were adopted.

The Board is committed to modernizing its standards, and this document requests information and comment from the public to inform any staff recommendation to the Board regarding updates to the interim attestation standards, including possible consolidation or elimination of certain standards.

The PCAOB is committed to modernizing its existing standards and to issuing new standards where necessary in light of developments in auditing and the capital markets. In that regard, the Board is considering updating its interim standards1 related to attest engagements ("PCAOB attestation standards").

Registered public accounting firms are sometimes engaged to examine and report on matters outside of an audit of financial statements.

These engagements include examination, review, and agreed-upon procedures engagements, which involve issuing a report on subject matter, or an assertion about subject matter, that is the responsibility of another party ("attest engagements").

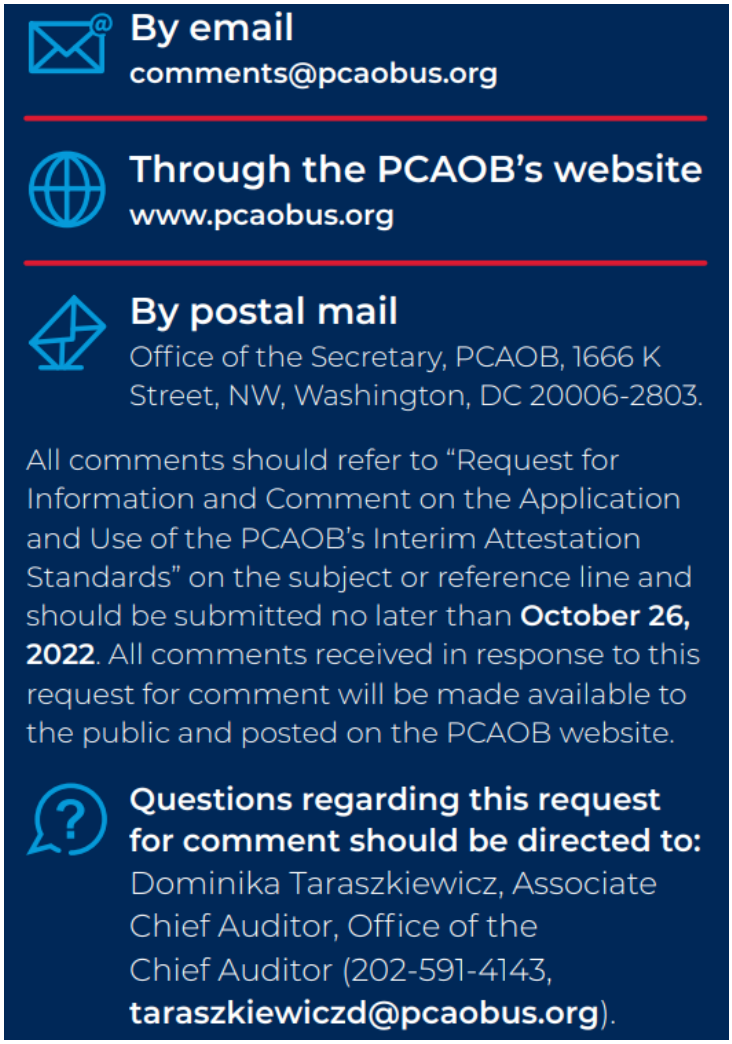
The subject matter of an attest engagement can vary and may relate to, for example, a company's compliance with laws and regulations, or a company's historical data or measures that are evaluated against certain criteria.

An attest engagement performed under PCAOB standards is designed to provide a certain level of assurance (as described below) and involves issuing a corresponding report ("attestation report"):

- Examination attest engagements provide reasonable assurance;

- Review attest engagements provide moderate assurance; and

- Agreed-upon procedures attest engagements do not provide specific assurance but involve a report on the performance of specified procedures and the resulting findings.



To read more: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/standards/staff-request-for-comment/rfc-application-use-interim-attestation-standards.pdf?sfvrsn=fd791256_2

BIS Working Paper No 1039

Cyber risk in central banking

by Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros and David Whyte - Monetary and Economic Department

The rising number of cyber attacks in the financial sector poses a threat to financial stability and makes cyber risk a key concern for policy makers.

This paper presents the results of a survey among members of the Global Cyber Resilience Group on cyber risk and its challenges for central banks.

The survey reveals that central banks have notably increased their cyber security-related investments since 2020, giving technical security control and resiliency priority.

Central banks see phishing and social engineering as the most common methods of attack, and the potential losses from a systemically relevant cyber attack are deemed to be large, especially if the target is a big tech providing critical cloud infrastructures.

Generally, respondents judge the preparedness of the financial sector for cyber attacks to be inadequate. While central banks in most emerging market economies provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in advanced economies do.

Cooperation among public authorities, especially in the international context, could improve central banks' ability to respond to cyber attacks.

The survey reveals four main insights.

First, central banks from AEs and EMEs differ in their assessment of the frequency and cost of different cyber attacks. All central banks deem phishing and other forms of social engineering as the most likely type of attack vectors. AE central banks are significantly more worried about supply chain attacks than their EME counterparts.

When it comes to the costs resulting from an attack, advanced persistent malware and ransomware attacks rank highest. Turning to the who of these attacks, AE central banks deem organised crime and state-sponsored entities to be the main perpetrators. Among EME central banks, it is organised crime and individuals or activists.

Second, central banks actively discuss and develop policy responses to cyber attacks and have increased their cyber security-related investments notably since 2020.

Technical security control and resiliency feature high on the priority list in terms of areas for investment in cyber security.

Training existing staff on cyber security or hiring new staff with the relevant skills are also considered important, especially among EME central banks. Beyond investments, central banks focus on developing concrete policy responses.

All central banks put a high focus on developing an incident response plan in case their own institution is attacked, and several central banks are also developing a formal strategy for responding to an attack on the financial system at large.

All central banks run internal exercises to simulate cyber attacks, and the most frequently modelled scenarios are an attack on the system of the central bank itself, as well as an outage of the payments system or other critical FMI.

While supervisory authorities in most EMEs provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in AEs do.

Similarly, while supervised firms are mandated to report losses related to cyber attacks to the central bank in almost all EMEs, only two-thirds of AE respondents report that such disclosure is required.

No jurisdiction requires firms to disclose such losses publicly, however.

Third, central banks deem the potential losses from a systemically relevant cyber attack to be large, and think that losses from cyber attacks in the financial sector have increased over the past year.

Only a few central banks fully agree that the financial sector is adequately prepared for cyber attacks, and over half of the respondents think that investment in cyber security has been inadequate over the past year.

Beyond traditional financial institutions, respondents reported that they see fintechs to be more at risk from a cyber attack than big techs, even though most respondents agree that a successful attack on a big tech would lead to materially higher aggregate costs than an attack on a fintech.

And **fourth,** central banks in AEs and EMEs already cooperate widely on a range of topics. Bilateral cooperation among central banks, as well as cooperation in bodies at the regional and global levels, is the norm.

When it comes to specific topics related to cooperation, information sharing, simulations and policy formulations to improve cyber resilience stand out in AEs. Among EMEs, central banks frequently cooperate in the realms of information sharing and policy formations.

In addition, over two-thirds of respondents develop common standards and protocols for the financial sector.

The BIS supports central banks' cyber security work, as well as global cooperation in this domain, in several ways – for example, through its Cyber Resilience Coordination Centre or projects of the BIS Innovation Hub.

To read more: https://www.bis.org/publ/work1039.pdf

BINDING OPERATIONAL DIRECTIVE 23-01

A web-friendly version of the *Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks*.

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.

Section 3553(b)(2) of title 44, U.S. Code, authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives. Federal agencies are required to comply with these directives.

These directives do not apply to statutorily defined "national security systems" or to certain systems operated by the Department of Defense or the Intelligence Community.

This directive refers to the systems to which it applies as "Federal Civilian Executive Branch" systems, and to agencies operating those systems as "Federal Civilian Executive Branch" agencies.

Background

Continuous and comprehensive asset visibility is a basic pre-condition for any organization to effectively manage cybersecurity risk.

Accurate and up-to-date accounting of assets residing on federal networks is also critical for CISA to effectively manage cybersecurity for the Federal Civilian Executive Branch (FCEB) enterprise.

The purpose of this Binding Operational Directive is to make measurable progress toward enhancing visibility into agency assets and associated vulnerabilities.

While the requirements in this Directive are not sufficient for comprehensive, modern cyber defense operations, they are an important step to address current visibility challenges at the component, agency, and FCEB enterprise level.

The requirements of this Directive focus on two core activities essential to improving operational visibility for a successful cybersecurity program: asset discovery and vulnerability enumeration.

- **Asset discovery** is a building block of operational visibility, and it is defined as an activity through which an organization identifies what network addressable IP-assets reside on their networks and identifies the associated IP addresses (hosts).

  Asset discovery is non-intrusive and usually does not require special logical access privileges.

- **Vulnerability enumeration** identifies and reports suspected vulnerabilities on those assets. It detects host attributes (e.g., operating systems, applications, open ports, etc.), and attempts to identify outdated software versions, missing updates, and misconfigurations.

  It validates compliance with or deviations from security policies by identifying host attributes and matching them with information on known vulnerabilities.

  Understanding an asset's vulnerability posture is dependent on having appropriate privileges, which can be achieved through credentialed network-based scans or a client installed on the host endpoint.

Discovery of assets and vulnerabilities can be achieved through a variety of means, including active scanning, passive flow monitoring, querying logs, or in the case of software defined infrastructure, API query.

Many agencies' existing Continuous Diagnostics and Mitigation (CDM) implementations leverage such means to make progress toward intended levels of visibility.

Asset visibility is not an end in itself, but is necessary for updates, configuration management, and other security and lifecycle management activities that significantly reduce cybersecurity risk, along with exigent activities like vulnerability remediation.

The goal of this Directive is for agencies to comprehensively achieve the following outcomes without prescribing how to do so:

- Maintain an up-to-date inventory of networked assets as defined in the scope of this directive;

- Identify software vulnerabilities, using privileged or client-based means where technically feasible;

- Track how often the agency enumerates its assets, what coverage of its assets it achieves, and how current its vulnerability signatures are; and

- Provide asset and vulnerability information to CISA's CDM Federal Dashboard.

Agencies may request CISA's assistance in conducting an engineering survey to baseline current asset management capabilities. CISA will work with requesting agencies to provide technical and program assistance to resolve gaps, optimize scanning, and support achieving the required actions in this Directive.

To read more: https://www.cisa.gov/binding-operational-directive-23-01

https://www.cisa.gov/implementation-guidance-binding-operational-directive-23-01

BINDING OPERATIONAL DIRECTIVE 23-01 Questions and Answers

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Frequently Asked Questions

Q: What is the scope of this directive? Which devices specifically need to be scanned?

A: This directive applies to all IP-addressable networked assets that can be reached over IPv4 and IPv6 protocols.

An IP-addressable networked asset is defined as any reportable (i.e., non-ephemeral) information technology or operational technology asset that is assigned an IPv4 or IPv6 address and accessible over IPv4 or IPv6 networks, regardless of the environment in which it operates.

The scope includes, but is not limited to, servers and workstations, virtual machines, routers and switches, firewalls, network appliances, and network printers — whether in on-premises, roaming, or cloud-operated deployment models.

The scope excludes ephemeral assets such as containers and third-party managed software as a service (SaaS) solutions.

Q: How does the pre-existing requirement to perform endpoint detection and response (EDR) differ from the requirements of this BOD? To what extent does EDR address asset visibility needs?

A: Asset visibility is a prerequisite for determining where to deploy EDR. While most EDR tools do not provide vulnerability information, the directive gives agencies the flexibility to use any tool that provides credential or client-level vulnerability information.

If an agency deploys EDR tools that can provide vulnerability information, those tools can be used in place of a client-based scanner.

Q: This BOD uses the term "networked assets." Does that imply cloud is out of scope?

A: Any non-ephemeral asset with an IP address is in scope, including applicable cloud assets. Many cloud use cases are unique. Many agencies have SaaS instances where agencies are unable to run their own scans.

In the case of traditional data center collocations, infrastructure as a service (IaaS), and in some cases platform as a service (PaaS), all assets with an IP address are in scope.

The scope excludes ephemeral assets such as containers and third-party managed SaaS solutions.

Q: Why does the directive say "initiate scans" instead of "execute" or "complete scans"?

A: Sometimes, especially in large enterprises, vulnerability scans may not be complete within the 14-day timeframe required in the BOD.

To overcome this issue, BOD 23-01 requires agencies to initiate a new scan every 14 days regardless of whether the previous scan has completed. Agencies are also required to feed available results for the previous scan three days after the new scan is initiated, even when the previous scan is not fully complete.

Q: What is the difference between "asset management" and "asset discovery"?

A: Asset management and asset discovery are two distinct activities that frequently go hand in hand.

Asset management is the active monitoring and administration of endpoints using a centralized solution, such as unified endpoint management (UEM), mobile device management (MDM), or enterprise mobility management (EMM).

Inventories from asset management solutions may be used to feed the information about agency assets into the results of a comprehensive asset discovery effort.

Asset discovery is the process of checking an IPv4 or IPv6 network for active and inactive hosts (e.g., networked assets) by using a variety of methods. The most common discovery methods include actively trying to communicate with all IP addresses in a range using a scan tool such as **"nmap"** (which is only feasible on smaller IPv4 based networks), or by passively monitoring traffic on the wire to detect activity from any new assets.

Asset discovery helps organizations find unmanaged assets that are present on the network to ensure they are brought under appropriate management.

It also helps organizations identify networked devices, such as Internet of Things (IoT), that cannot be centrally managed. It is possible for an asset to fall off the management tool due to inactivity or other reasons, requiring it to be rediscovered.

Q: Why does the directive reference the software bill of materials (SBOM) in the Background section but not in subsequent sections?

A: SBOM is mentioned in the introduction to convey the Administration's vision and describe our desired state in the long term.

The directive focuses on very specific first steps that can be achieved within the next 6-12 months and are prerequisites for broader adoption of SBOM.

Without comprehensive asset management, agencies will be unable to effectively use SBOMs to manage risk posed by asset components or libraries.

Q: We offer public wireless access in conference rooms and lobbies. Are guest networks in scope?

A: Guest hosts are not in scope, provided the guest networks are physically segmented from agency networks.

Q: Are bring-your-own-device (BYOD) assets in scope?

A: Most federal agencies do not allow BYOD on enterprise networks. If they do, then BYOD devices are in scope.

This does not apply to personally owned equipment that connects to federal networks via web interface (e.g., website visitors or remote users connecting via SSL remote access solutions).

Q: Are air-gapped networks in scope? It may not be possible to transfer a signature to air-gapped networks within 24 hours.

A: Many logically isolated networks and systems are incorrectly considered air-gapped. Any device, system, or network that is directly connected to the operating environment, or is connected to another system that is connected to the operating environment, is not considered air-gapped and is in scope for BOD 23-01. Only systems that are truly physically air-gapped are out of scope.

Q: Does the BOD include requirements for scanning software and configuration enumerations?

A: No, the BOD requirements address only basic (IP) asset discovery and vulnerability enumeration.

The current BOD does not address hardware management, software management, or configuration management and associated controls.

Note that some vulnerabilities due to misconfigurations and basic configurations may be captured by standard vulnerability scanners.

Q: Which cloud assets are in scope?

A: Agencies are responsible for the discovery and enumeration of networked assets under agency control, such as assets in authority-to-operate (ATO) inventories.

Each cloud instance is unique, but in general, third-party hosting solutions where agencies still control physical or virtual hosts, such as infrastructure as a service, are within the scope of this directive.

Q: Are communications devices, such as IP telephony, VOIP phones, cameras, and unified communications peripherals in scope?

A: Yes, these devices are in scope. Adversaries have specifically targeted these devices as they are typically more difficult to harden.

Glossary

Vulnerability enumeration performance data – Otherwise referred to as scanning logs, vulnerability enumeration performance data describes datapoints or measurements that provide visibility on the level of performance relative to the requirements in this directive, using automation and machine-level data (e.g., logs/events indicating successful credentialed enumeration completion, date/timestamps surrounding enumeration activities, and signature/plug-in update date/timestamps). Data requirements to satisfy this objective will be published in a common data schema and made available to every Federal agency.

Vulnerability enumeration – A technique to list host attributes (e.g., operating systems, applications, and open ports) and associated vulnerabilities. Vulnerability enumeration typically requires privileged access to gain full visibility at the application and configuration levels.

Privileged credentials – A local or network account or a process with sufficient access to enumerate system configurations and software components across an entire asset. Administrators must apply the principle of least privilege and/or separation of duties on the accounts used for vulnerability enumeration. Poisoning and machine-in-the-middle type attacks commonly target accounts with elevated privileges, including those used for vulnerability enumeration.

Roaming devices – Devices that leave an agency's on-premises networks, connect to other private networks, and directly access the public internet.

Nomadic devices – Devices that permanently reside outside of agency networks.

To read more: https://www.cisa.gov/binding-operational-directive-23-01

https://www.cisa.gov/implementation-guidance-binding-operational-directive-23-01

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.

Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: https://www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: https://www.sarbanes-oxley-association.com/Reading_Room.htm

3. Training and Certification - You may visit: https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We tailor all programs to meet specific requirements.