



U.S. Cyber Market Outlook

Helping you come
through for your clients





The U.S. cyber insurance market is at a standoff. As coverage demand continues to accelerate in 2021, coverage supply has put on the brakes. On the demand side are organizations of all sizes, across all industry classes. They are looking to make an initial coverage purchase, increase their existing coverage or simply renew within budget.

On the other side are the insurance companies. They have been battered by higher-than-anticipated losses, so they are only willing to write less coverage (or sometimes no coverage) at a significantly higher rate. Caught between the two is the insurance broker, who faces new challenges in bringing both parties together.

“Over the past year, we’ve seen the challenges of the COVID-19 pandemic and increasing frequency and severity of ransomware attacks put pressure on the U.S. cyber liability market,” stated Steve Robinson, Risk Placement Services (RPS) area president and national cyber practice leader. “While this market dynamic developed quickly, within a matter of months, long-standing underwriting issues in this market, as well what had been a growing mismatch between exposures and underwriting, helped to create the current situation and the imbalance between coverage supply and demand.”

To understand how the cyber insurance market got to its current place, it’s useful to look at how this market has evolved.

A WORK IN PROGRESS

The cyber insurance market, which is approaching its 25th anniversary, is still relatively young compared to other property and casualty coverages.

Since the first internet security liability policy was underwritten in the mid-1990s, the market has grown and expanded beyond the information technology (IT) companies that the original policies were marketed to.

The early cyber insurance policies were essentially an errors & omissions form for a technology company. They typically covered named perils such as unauthorized access, data destruction or a virus.

In the mid-2000s, cyber insurers began offering first-party expense coverage to protect the entity itself. That increased the pool of potential cyber insureds to any organization that used technology.

“In those early days, I would often talk with agents about how cyber coverage was becoming a must-have coverage similar to general liability,” recalled April Solano, area assistant vice president at RPS. “It was clear that for many

companies, their liability was moving from the real world to cyber space. Today’s digital workplace has deepened and expanded cyber exposures.”

As the use of technology in the workplace grew, the line between tech and non-tech companies began to blur. Data breach notification laws, which first went into effect in California in 2003, were another factor that drove demand for cyber coverage.

“Data breach notification laws brought this exposure front and center for many companies,” observed Nick Carozza, area vice president, RPS. “They often viewed their cyber coverage less as insurance and more as access to a vetted group of service providers that would help them recover from the impact of a data breach. At that time, the cost per record for data breach notification was one of the most common coverage questions we would receive from retail brokers.”

Growing in tandem with data breach was social engineering. Hackers use social engineering tactics to gain access to network credentials or other information that will allow them to carry out their crimes, undetected.

According to one technology firm, only 3% of malware enters a company’s network through a technical flaw. The other 97% is through a social engineering scheme.¹

Business email compromise (BEC) is a popular type of social engineering. In the early years this was often referred to as “whaling” because an employee would receive an email from the company’s CEO or other C-suite executive. Now typically, an employee receives an email from a vendor, a customer or even a colleague, which asks them to pay an invoice or change their payment method. BEC complaints have grown steadily over the years, both in terms of incident number and cost.

The FBI’s Criminal Crime Complaint Center victim/complaint count grew from 1,495 in 2014 to 19,369 in 2019. Similarly, the associated losses jumped from \$60.3 million in 2014 to \$1.8 billion in 2019.²

Insurance companies were more than eager to meet this growing demand for coverage. Competition among carriers drove down premiums. Insurance companies turned easy underwriting standards into a competitive advantage. Direct written premium (combined monoline and package) grew steadily, reflecting demand and growing capacity rather than demand and rising rate.

As both cyber insurance supply and demand boomed, so did claims. Data breaches continued to grow, reaching a peak in 2017 with 1,632 data breaches, exposing more than 197 million records.³ However, with the exception of a few large data breaches aimed at retailers and healthcare organizations, the claims were relatively modest.

INDUSTRY’S STANDALONE CYBERSECURITY LOSS RATIOS SOARED IN 2020



Source: S&P Global Market Intelligence



Not All Speaking the Same Language

One of the challenges of the cyber insurance market is the significant variations between insurance companies in terms of their appetite, limits and policy forms. Inconsistencies in how different insurance companies refer to the same type of coverage can make a complex coverage even more confusing. Here are some examples:

- Social engineering vs. cyber deception
- Extortion vs. ransomware
- Bricking vs. computer hardware replacement costs
- Phishing vs. invoice manipulation

“At that time there was a lot of capacity in the cyber insurance market,” observed Adam Connor, area senior vice president at RPS. “The marketplace was growing yet the loss ratios weren’t. Unfortunately underwriting didn’t correctly anticipate how quickly this situation could change.”

A TURN FOR THE WORSE

The market suddenly changed direction in 2020 as insurance companies began to calculate the unanticipated impact of ransomware claims on their bottom line. The additional exposure created by employees working from home during the global pandemic contributed to their greater focus.

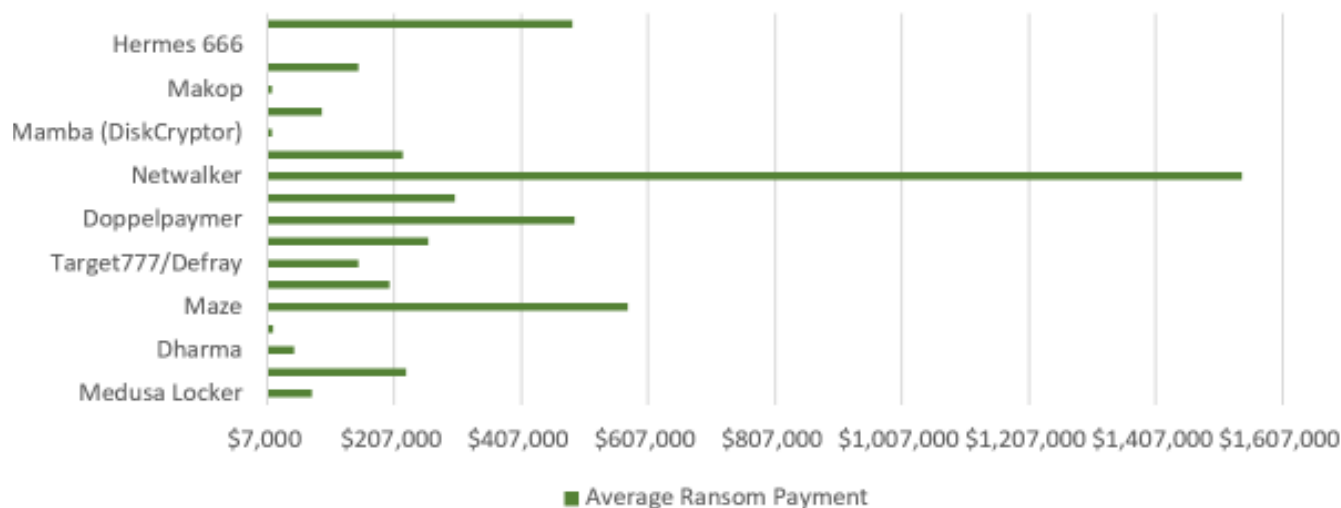
Within a single year, claim frequency and severity had climbed at an unprecedented rate. Losses often far exceeded actuarial estimates. Cyber loss ratios jumped from 44.8% in 2019 to 67.8% in 2020, and higher for many carriers.⁴

Claims for cyber-induced business interruption (BI) began to soar. Supply chain-related BI claims, resulting from a data breach at a third party, also became more common.

Capacity restrictions started to grip the market. Cyber insurance companies, which relied more on risk transfer through reinsurance than more established property & casualty markets, began to feel the squeeze from their reinsurers.

“With cyber liability loss ratios climbing, even with demand increasing and premiums climbing reinsurers began to curtail how much in premium insurance companies could layoff with them,” said Robinson. “Some markets discovered that they reached their risk transfer ceiling with their reinsurer faster than anticipated. They found themselves in a situation where the shelves were empty and there was no reinsurance left to buy.”

RANSOMWARE VARIANTS MAKE A RANGE OF REQUESTS



Source: Kivu (in partnership with Hiscox)

Study: Trends in Ransomware and Doxing H1 2020 Review

These unanticipated reinsurance constraints were reflected in the available underwriting capacity from several markets.

Insurers that were more than eager to issue \$5 million cyber liability policies in 2020 have scaled back to limits of \$1-3 million, even on a renewal. As a result, building a cyber liability coverage tower has also become more challenging.

THE RANSOMWARE EPIDEMIC

While cyber liability exposures continue to evolve beyond data breach and social engineering, by 2018, ransomware was beginning to raise the stakes considerably. Between midyear 2018 and 2019, ransomware attacks multiplied, growing 500%, which can lead organizations to pay the ransom, according to Forrester.⁵ They also became more targeted, aimed at a handful of organizations or increasingly, just one.

“The days of denial of service ransomware involving botnets and hundreds or thousands of dollars demands are long gone,” noted Dillon Behr, area vice president at RPS. “Today’s ransomware attacker is more targeted and sophisticated. It’s no longer someone sitting in their basement waiting to see how many random companies will respond to their threat.”

“This year, agents are scrambling to build towers that offer their customers the same limits of liability that they’ve had in previous years,” observed Solano. “A \$10 million tower built with five insurance companies in 2020, might now require 10 companies in 2021.”

Even though both are forms of cyber extortion, ransomware differs from a data breach in several important ways.

Unlike a data breach, ransomware is an industry agnostic exposure.

Because ransomware relies more on a company’s willingness to pay for access to its critical data, rather than how much personally identifiable information (PII) it holds, the pool of potential targets has expanded to include nearly every organization in the U.S.

Small-to-midsize enterprises have become a viable target, as what matters is their willingness to pay, rather than their corporate revenues.

Paying for a decryption key is just one part of the cost of ransomware. Other costs include the time and money required to make sure that the data is restored properly. Attackers are also increasingly including a payment demand to prevent the release of customer data and nonpublic information. “Ransomware has become a two-headed monster,” commented Robinson, “Double extortion, as it’s known, has become a contributing factor in cyber claim severity over the past year.”

UNDERWRITING TRANSFORMATION

In response to these market conditions, cyber insurance underwriting has become more reflective of today’s risks.

While the days of an application with a handful of questions are over, this also doesn’t mean a return to the 10+ page application forms. Instead the questions have become more strategic and better reflect the current cyber exposures.

Even on renewals, insurance companies have begun asking detailed questions about a company’s information security safeguards and practices through supplemental application forms for ransomware and BI.

Network security questions now go beyond antivirus software and requests for the latest version of the company’s data privacy policies to include topics such as:

Because of the potential impact of ransomware following the Colonial Pipeline attack in June 2021, the U.S. Department of Justice elevated ransomware investigations to the same priority level as terrorism.

That same month, the FBI requested a \$40 million increase for its cybersecurity budget for the next fiscal year due to the increasing frequency and severity of ransomware attacks.

- Data backup, segregation, testing and recovery
- Storage of biometric information for companies that use fingerprint scans
- IT vendor vetting process and management controls
- Employee cybersecurity training
- Remote desktop protocol (RDP)
- Endpoint detection and response (EDR)
- Email security
- Log-in security and user authentication.

Manufacturing Moves from Low to High Risk

When a data breach was the primary cyber exposure, manufacturing companies were considered to be a relatively low-risk industry class.

Unlike retailers and healthcare organizations, which are a treasure chest of personally identifiable information (PII), manufacturing companies weren’t that attractive as a data breach target. And the majority of the employees weren’t sitting at their desks checking email all day, making them also less susceptible to social engineering.

The automation of the manufacturing process has increasingly brought technology onto the shop floor. Therefore, ransomware has made manufacturing a hot target with the sector now accounting for 11% of all cybercrimes.*

While the advanced technology has made manufacturing companies more productive and globally competitive, it has also increased the number of potential entry points for a hacker. For example, a piece of equipment that utilizes software connected to the internet can provide a hacker with a gateway to a company’s corporate network.

Because of the significant business interruption and related supply chain issues, manufacturers that lack the proper backup safeguards tend to be more likely to pay a ransomware request. As a result, cyber claims are higher, both in terms of frequency and severity, within this sector.

*Baker Hostetler 2020 Data Security Incident Response Report.



Insurance companies are setting IT infrastructure minimums. What has been a challenge for many companies is that these controls went into effect so quickly.

“Insurance companies are setting IT infrastructure minimums,” explained Carozza. “What has been a challenge for many companies is that these controls went into effect so quickly. Many companies were caught in a situation where they didn’t have the time or the funds to implement these controls before their policy renewal date.”

Multi-factor authentication (MFA) in particular has become a must-have to qualify for cyber coverage, as it’s one of the most effective ways to prevent either a cybercrime or cyber extortion event.

MFA, which is also referred to as two-factor authentication, requires the user to provide at least two different verification methods to gain remote access to applications, servers or networks. For example, MFA requires users to present both a password and a corresponding device (such as a cell phone) to log into a network.

With MFA, if bad actors gain unauthorized access to an employee’s user names and passwords from the Dark Web, they won’t be able to access the network without that secondary factor.

Nearly all cyber insurance providers have added MFA as an underwriting requirement in 2021 as they focus on addressing deteriorating loss ratios.

While many insurance companies simply won’t underwrite, or even renew, a cyber policy for a company without MFA in place, others will instead apply sublimits or even exclusions on cyber extortion and BI resulting from ransomware events to control their loss ratios.

Connor believes it’s also important to consider how an insured will use MFA once it’s integrated into its network security.

“There’s a difference between just utilizing MFA for remote access when employees log in via VPN, vs. using it to secure privileged and administrative accounts and confidential information,” he stated.

The Crypto Connection

Hackers never make their ransomware demands in government-issued currency, instead requesting payment in cryptocurrency.

The anonymity built into blockchain, the digital ledger system that forms the foundation of bitcoin and other cryptos, is what makes them the currency of choice for hackers. Indeed, some cybersecurity experts believe that cryptocurrency use in ransom demands has helped to drive up the value of various cryptos.

The U.S. Treasury Department has taken notice of this trend. In September 2021, the department’s Office of Foreign Assets Control issued an update of its October 2020 advisory* highlighting the sanctions risks associated with ransomware payments.

*Ransomware Advisory:
<https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001>



Even with the right controls in place, organizations are finding it next to impossible to secure their 2021 coverage at 2020 rates.

Insurance companies are incorporating the same scanning technology used by hackers into their own underwriting process. This allows them to assess an organization's perimeter security and also develop a metric-based estimate for a potential cyber attack.

These scanning tools can be used to identify unused, vulnerable open ports that could provide a bad actor with a network entry point.

Tech-forward insurers are also incorporating artificial intelligence (AI) into the underwriting process.

However, even with the right controls in place, organizations are finding it next to impossible to secure their 2021 coverage at 2020 rates.

Carriers are strategically increasing premiums—and lowering coverage limits—on the industry classes that have been hit hardest by cybercrime and cyber extortion over the past year. These include, among others:

- Education
- Public entity/government
- Healthcare
- Construction
- Manufacturing

Companies and organizations in these industry classes have seen premium increases as high as 300% or more when they renew their cyber coverage.

THE WFH MIGRATION

While work-from-home (WFH) was a growing trend even before the pandemic, COVID-19-related office closings drove millions of U.S. employees to work from their homes. Many companies were focused more on getting their employees back up and running as fast, rather than as securely, as possible.

This situation created network vulnerabilities and widened the number of entry points for hackers. Bad actors were eager to take advantage of the pandemic's disruption of business operations.

Many link the explosion in ransomware to the migration of millions of employees from the office to their homes in March 2020.

Small businesses were hit by BEC related to the federal Paycheck Protection Program (PPP). Perpetrators would use publicly available information to identify PPP loan recipients and then send an email requesting sensitive information such as passwords, social security numbers and financial information.

Human behavior has always been the weakest link in cybersecurity and that has continued during the pandemic. Many employees let their guard down at home and use shortcuts such as sending work documents from a personal email account.

It is also easier for employees to download file sharing programs and other unauthorized software onto a corporate laptop.

Wire fraud and social engineering are also more likely to occur with WFH employees. In an office, an employee can easily ask colleagues if they've received a suspicious email or show it to them on their screen. With WFH, the safeguards created by those casual interactions no longer exist.

Home WiFi networks have also made it easier for scammers to access a corporate network as they often lack firewalls. The antivirus software on home routers is often out of date as well.

A CONSTANTLY EVOLVING MARKET

While the current market climate led a well-known credit rating agency to call its outlook for cyber insurance “grim,” those who are on the market’s front line are more optimistic and realistic about its long-term future. As Robinson said, this year’s changes in capacity, underwriting standards and even increases in premium were a “necessary evolution.” These changes should lead to most insurance companies having a more stable cyber book in the future.

Solano agrees that changes were necessary. “Insurance companies took steps this year, such as cutting limits and tightening underwriting controls, to ensure that they could keep writing cyber in the years ahead. We need these companies to be in it for the long haul with insureds,” she explained.

The number and mix of insurance companies offering cyber coverage may also shift.

Successfully entering the cyber insurance market today is more challenging and complex than it was two or three years ago. In certain ways, the insurtechs that have entered this market have a natural advantage. And traditional carriers are starting to follow these newcomers’ leads in incorporating scanning and additional AI-enabled technologies into the underwriting process.

Yet, the original entrants also have the benefit of greater volumes of historical claims data to help inform their future steps.

Human behavior has always been the weakest link in cybersecurity and that has continued during the pandemic.

Overcoming the Resistance to MFA

Insureds are often surprisingly reluctant to implement MFA. In many cases, a bit of client education can help break down that resistance. That’s a conversation worth having as MFA is one of the most effective cybersecurity tools readily available.

Research from Google showed that MFA can potentially block 99% of bulk phishing attacks and 66% of targeted attacks.*

MFA-resistant insureds often cite cost as a concern. Yet, depending on the level of security and the vendor, MFA costs start as low as \$3 a month per employee.


Even with the additional expense around onboarding and system maintenance, those costs pale in comparison to what an organization will ultimately pay if they have a cyber attack.

Insureds may also receive pushback on MFA from their employees. MFA can make the log-in process a bit more cumbersome as employees have to authenticate each time they log in.

Employees in certain industry classes, notably education, have pushed back on MFA, raising the point that if they’re using their personal devices to authenticate identification then their employer should pay for those devices.

Thankfully, technology providers are offering a wider variety of options for secondary authentication. These include tokens and biometric methods, such as fingerprints and facial scans—in addition to incorporating verification via call-backs using traditional phone lines.

*Google Security Blog, “New Research: How Effective Is Basic Account Hygiene at Preventing Hijacking,” accessed September 6, 2021.



Even when the balance between capacity supply and demand returns to equilibrium, sublimits on ransomware are expected to remain as a way to limit the impact of cyber extortion on insurers.

“Rather than simply declining to write business in this challenging market, insurance companies need to become better at determining what a good risk is, and write that business,” advised Behr. “Between premiums, sublimits and retentions, as well as a more thorough underwriting process involving network scans, insurance companies have a lot of levers to pull to profitably write this business.”

Even when the balance between capacity supply and demand returns to equilibrium, sublimits on ransomware are expected to remain as a way to limit the impact of cyber extortion on insurers. In many cases, the attackers are able to determine the ransomware limits in their victim’s cyber policy before they even make their demand. So lower ransomware sublimits may become viewed as a deterrent as well as a means of controlling loss ratios.

With the pressure from underwriters to raise their security standards, insured organizations will need to spend more on technology.

One study found that 55% of enterprise executives planned to increase their cybersecurity budgets in 2021 and 51% intended to add full-time staff.⁶ With this spend should come increased use of sophisticated network security solutions, such as Endpoint Detection and Response (EDR).

EDR provides real-time monitoring of the thousands of endpoints that make up the boundaries of a corporate network. EDR also incorporates machine learning to help detect and even eradicate threats in real time.

CONSIDERATIONS FOR AGENTS

Insurance agents need to keep pace with the constantly changing nature of technology, and the resulting exposures make cyber a tough market for retail agents to dabble in.

Agents need to stay on top of cyber insurers’ varying appetites, policy forms and language modifications. And capacity restrictions are making them work harder than ever.

While the technology jargon can be daunting, a good place for agents to begin their cyber education is by becoming familiar with application language around topics such as MFA and RDP, as well as proper back-up procedures and employee education programs. These are areas that can make or break a customer’s ability to receive coverage.

They should also tap into available expertise, whether it’s an agency colleague or a wholesale broker with significant expertise in this sector.



For renewals, preparing insureds for sticker shock can be a difficult yet important conversation to have. It's also important for agents to pay more attention than usual to renewal terms, conditions and sublimits, so that customers don't encounter surprises in the event that they have a claim.

CONSIDERATIONS FOR INSURED

The first step is to put a greater focus on network security. Smaller organizations or those in industry sectors such as construction and manufacturing that weren't traditional targets, need to stop thinking that their business is immune from a cyber attack, simply because they don't store thousands of customer credit card numbers or PII.

Carozza has some specific advice for small businesses and organizations. Given the pressures on smaller IT departments to keep pace, as well as their tendency to be more reactive than proactive, he recommends that these companies either consider outsourcing their network security to a third-party provider or at least augmenting their existing staff with outside expertise.

Employee education is another critical area for organizations to address. This needs to go beyond a yearly requirement for employees to watch a video and then pass a test. Organizations need to make training engaging and help employees feel that they are part of the solution. Tabletop exercises that require participants to work through different risk scenarios and potential cyber threats can be an effective way to accomplish that goal.

Nearly all cyber insurance providers have added MFA as a requirement for underwriting in 2021.



THE NEXT STAGE

Some view the current state of the cyber liability market as evidence of a market breakdown. A more positive and realistic perspective is that what we are experiencing is evidence of a functioning market.

Challenges such as MFA adoption are an opportunity for agents to demonstrate their value as a trusted advisor and help their clients reduce their risks. The drastic changes that have occurred in 2021 have served to better align the cyber liability underwriting process with the exposures.

A better balance between coverage supply and demand should follow through the end of 2021 and into 2022.

Many insureds need to take a more active role in protecting their organizations. Even the most robust cyber insurance policy is not a suitable substitute for poor information security practices. In addition to MFA, proper data backup and greater employee education and engagement are now cybersecurity must-haves for nearly every organization.

There is no question that the cyber liability market is challenging. And just as workplace technologies will continue to evolve, so too will cyber exposures.

While no one can predict what the next leading cause of cybersecurity attacks will be, there's little debate that bad actors are developing new threats as you read this report.

We believe the partnership between IT, government, insurance and private enterprise in combating cyber exposures is stronger than it has ever been. And it will need to remain strong if we are to continue to innovate in this increasingly critical coverage area.

Cyber threats are everywhere. They are constantly changing and affecting more businesses every day. RPS cyber experts have been leading the charge from the start and can help find coverage for cyber exposures of any size. RPS has helped countless businesses across a broad range of industries and continues to be a trusted partner in this most dynamic area of coverage.

CONTRIBUTORS

Steve Robinson, National Cyber Practice Leader

Adam Connor, Area Senior Vice President

Nick Carozza, Area Vice President

Dillon Behr, Area Vice President

April Solano, Area Assistant Vice President

ABOUT RISK PLACEMENT SERVICES

Risk Placement Services (RPS) is one of the nation's largest specialty insurance products distributors, offering solutions to independent agents and brokers in wholesale brokerage, binding authority, programs, standard lines and nonstandard auto. The RPS team, fueled by a culture of teamwork, creativity and responsiveness, works with top-rated admitted and non-admitted carriers to design robust coverage for clients through its more than 80 branch offices nationwide.

For more information, visit RPSins.com.

¹KnowBe4, <https://www.knowbe4.com/what-is-social-engineering/>, accessed August 27, 2021.

²Broadcom, "BEC Scams Remain a Billion-Dollar Enterprise," July 23, 2019, accessed August 26, 2021 and FBI, "Internet Crime Report 2020," p. 10.

³Statista, "Annual Number of Data Breaches and Exposed Records in the United States," March 3, 2021. Accessed August 25, 2021.

⁴AM Best, "Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk," June 2, 2021.

⁵Forrester Research, "Forrester's Guide to Paying Ransomware," June 5, 2020.

⁶PwC, "Global Digital Trust Insights 2021, October 5, 2020.

The information contained herein is offered as insurance Industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer legal advice or client-specific risk management advice. Any description of insurance coverages is not meant to interpret specific coverages that your company may already have in place or that may be generally available. General insurance descriptions contained herein do not include complete Insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis.

Copyright © 2021 Risk Placement Services, Inc. No copyright claimed in works of the U.S. Government.

RPS40957 0921