Hillary Clinton Made More in 12 Speeches to Big Banks Than Most of Us Earn in a Lifetime

Zaid Jilani
Jan. 8 2016, 1:28 p.m.
Democratic presidential candidate Bernie Sanders this week assailed rival Hillary Clinton for taking large speaking fees from the financial industry since leaving the State Department.

According to public disclosures, by giving just 12 speeches to Wall Street banks, private equity firms, and other financial corporations, Clinton made $2,935,000 from 2013 to 2015:

**Clinton Made $2.9 Million From 12 Speeches To Big Banks**

<table>
<thead>
<tr>
<th>Financial Firm</th>
<th>Money Made In Paid Speeches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ameriprise</td>
<td>$225,000</td>
</tr>
<tr>
<td>Apollo Management Holdings</td>
<td>$225,000</td>
</tr>
<tr>
<td>Bank of America</td>
<td>$225,000</td>
</tr>
<tr>
<td>Canadian Imperial Bank of Commerce</td>
<td>$150,000</td>
</tr>
<tr>
<td>Deutsche Bank</td>
<td>$485,000</td>
</tr>
<tr>
<td>Fidelity Investments</td>
<td>$225,000</td>
</tr>
<tr>
<td>Golden Tree Asset Management</td>
<td>$275,000</td>
</tr>
<tr>
<td>Goldman Sachs</td>
<td>$675,000</td>
</tr>
<tr>
<td>Morgan Stanley</td>
<td>$225,000</td>
</tr>
<tr>
<td>UBS</td>
<td>$225,000</td>
</tr>
</tbody>
</table>

Clinton’s most lucrative year was 2013, right after stepping down as secretary of state. That year, she made $2.3 million for three speeches to Goldman Sachs and individual speeches to Deutsche Bank, Morgan Stanley, Fidelity Investments, Apollo Management
Holdings, UBS, Bank of America, and Golden Tree Asset Managers.

The following year, she picked up $485,000 for a speech to Deutsche Bank and an address to Ameriprise. Last year, she made $150,000 from a lecture before the Canadian Imperial Bank of Commerce.

To put these numbers into perspective, compare them to lifetime earnings of the median American worker. In 2011, the Census Bureau estimated that, across all majors, a “bachelor’s degree holder can expect to earn about $2.4 million over his or her work life.” A Pew Research analysis published the same year estimated that a “typical high school graduate” can expect to make just $770,000 over the course of his or her lifetime.

This means that in one year – 2013 – Hillary Clinton earned almost as much from 10 lectures to financial firms as most bachelor’s degree-holding Americans earn in their lifetimes – and nearly four times what someone who holds only a high school diploma could expect to make.

Hillary Clinton’s haul from Wall Street speeches pales in comparison to her husband’s, which also had to be disclosed because the two share a bank account.

“I never made any money until I left the White House,” said Bill Clinton during a 2009 address to a student group. “I had the lowest net worth, adjusted for inflation, of any president elected in the last 100 years, including President Obama. I was one poor rascal when I took office. But after I got out, I made a lot of money.”

The Associated Press notes that during Hillary Clinton’s time as
secretary of state, Bill Clinton earned $17 million in talks to banks, insurance companies, hedge funds, real estate businesses, and other financial firms. Altogether, the couple are estimated to have made over $139 million from paid speeches.

Top photo: Hillary Clinton with Goldman Sachs chief Lloyd Blankfein at a Clinton Global Initiative event, September 2014, in New York City.

CONTACT THE AUTHOR:

Zaid Jilani
✉ zaid.jilani@theintercept.com
✓ @ZaidJilani
Tuesday, August 11, 2015

HILLARY & BILL SHILL FOR A SECRET INTELLIGENCE AGENCY CARTEL

BILL'S EXECUTIVE ORDERS CREATED A WHITE HOUSE SPY-AGENCY CONTROLLED BY WALL STREET & SILICON VALLEY; QUEEN HILLARY IS ABOVE THE LAW

MORE BREAKING NEWS, AUG. 16, 2015:
BILL & HILLARY FIDELLED WHILE ROME BURNED IN 2008

NEW: OBAMA'S FREUDIAN SLIP IN EXECUTIVE ORDER 13691, FEB. 13, 2015
Barack Obama revealed his pathology that Executive Orders and American law are not the same. In giving more private crony tech company access to his spy-state machine, he stated in Sec. 8(a)(i): ‘Nothing in this order shall . . . impair . . . the authority granted by law or Executive Order . . .’ Former Clinton advisor, James P. Chandler, continues his secret re-write of the Constitution.

Between 2001-2015, Bill & Hillary gave 75 speeches to members of IBM's The Eclipse Foundation—the technology behind White House spy-state surveillance that was stolen from Ohio innovator Leader Technologies by Professor James P. Chandler, Leader's attorney and Clinton's adviser. Up to the 2008 banking crisis, Bill Clinton was paid $4 million for 26 speeches to Eclipse members. In 2008, Bill gave only one Eclipse speech on Nov. 15, 2008 to AWD Holdings—this was 11 days after Obama's election and eight days before Larry Summers assumed bank bailout control. Summers immediately gave $13 billion to Goldman Sachs.

NEW: OBAMA'S EXECUTIVE ORDER SHELL GAME
On Feb. 13, 2015, Obama issued Executive Order 13691 to help his BM Eclipse private sector spy-state cronies. Buried in Sec. 5(g) is an amendment to EO 12829 that designates EO 12356 (Apr. 6, 1982) as the new authority. However, EO 12356 was revoked on Oct. 14, 1995 according to EO 13292, Sec. 6.2(d)—during the time of the hearings for Chandler's FIG. 1—BILL CLINTON. On Nov. 15, 2008, Bill flew to Germany a week after Obama's election to collect a $450,000 speaking fee from his financial planner. AWD Holdings AG is a personal financial planner with no business in the U.S., now called Swiss Life. The $450,000 fee is his largest ever reported. A week later, Obama appointed Lawrence 'Larry' Summers, Bill's former Treasury Secretary, to oversee the bank bailout. Summers protégés, Sheryl K. Sandberg and Russian oligarch Yuri Milner, figure prominently in the Facebook spy-state surveillance platform. AWD wrote in 2008 that the U.S. banking crisis 'strengthened us.' This trading on inside knowledge is evident. Exploitation of children by the spy-state is clearly not an issue for the ambitious couple.

Click here for Hijack of the Cyber World Timeline and Database

Updated Nov. 13, 2015

More
Next
Blog» Create Blog Sign In
Economic Espionage Act. Obama also cites the wrong date for EO 12356 (Apr. 2, 1982). These built-in ambiguities ensure that ALL interpretations of the order will return to its author, James P. Chandler, our secret, unelected and unaccountable spy-state master. Confused yet? Precisely.

CONGRESS CONTACT LOOKUP

FINANCIAL HOLDINGS OF OBAMA POLITICAL APPOINTEES, BY AGENCY

BLOG ARCHIVE (New, 1/20/14)

UPDATE MAR. 25, 2014

FIVE critical AFI posts on judicial compromise

FULLY updated Mar. 25, 2014 in the wake of the Scribd censorship:

See 2008 Clinton Timeline. In 2010, Bill made $2.2 million for 11 Eclipse speeches. In 2012 (the year Facebook went public), Bill made $1.2 million for 16 Eclipse speeches. One 2012 speech was to Facebook's attorney, White & Case LLP. (On Dec. 5, 2008, Obama picked another Facebook attorney from Cooley Godward LLP, Donald K. Stern, to help him pick judges, one of whom was the last-minute replacement judge in Leader v. Facebook. Leonard P. Stark, who as a rookie muscled out 25-year veteran, Joseph J. Farman.) His 2012 speeches also included six Facebook underwriters (JPMorgan, Goldman Sachs, UBS, Deutsche Bank, Bank of America and Vanguard. See Clinton-Eclipse Speech Map below.

BREAKING NEWS, AUG. 15, 2015:

HILLARY WIPED SERVERS—JAMES P. CHANDLER WROTE BILL'S SECURITY RULES IN 1995

On Aug. 13, 2015, Hillary Clinton just turned over an empty private email server to the Justice Department. However, the Justice Department is not impartial since they had oversight of Hillary's activities, along with Hillary herself, as Secretary of State.

On Apr. 17, 1995, Bill Clinton’s national security confidante, Professor James P. Chandler, drafted Executive Order No. 12958—Classified National Security Information. Successive Presidents cite back to this order in dozens of related orders, so it governs Hillary Clinton’s current email server conduct. Section 6.1(b) authorizes the Attorney General to interpret the Order. Sec. 5.4(a) established the Secretaries of State & Defense, Attorney General, C.I.A. Director and two Presidential aides as oversight. If the principals are colluding, then accountability is non-existent.

Truly, the foxes are guarding the White House hen house.

ORIGINAL POST

(AUG. 12, 2015) — How many laws can Hillary Clinton break and stay out of jail? (Memo to Saul Alinsky’s Useful Idiots: Hillary & Bill are above the law, by Executive Order.)

ANSWER: Husband Bill issued Executive Order No. 13130 on Jul. 14, 1999 called the National Infrastructure Assurance Council (NIAC) to “enhance the partnership of the public and private sectors in protecting our infrastructure.”

New investigations reveal that Hillary relies on a string of Executive Orders related to NIAC that have been promulgated by her husband and his successors to protect herself from liability. Apparently, she hopes Saul Alinsky’s army of “Useful Idiots” (the unthinking American public) will forgive her and vote for her anyway.

BILL STARTED A WHITE HOUSE SPY AGENCY THAT WRITES ITS OWN RULES—WITHOUT CONGRESS

These national security Executive Orders set up a private intelligence agency operating out of the White House. The C.I.A. is subservient to it, so is the NSA, FBI, DIA, NRO...all U.S. intelligence operations.

ECONOMIC ESPIONAGE ACT—EXECUTIVE ORDER 12356

On Aug. 13, 2015, Hillary Clinton just turned over an empty private email server to the Justice Department. It is a matter of public record that the Justice Department is not impartial since they had oversight of Hillary’s activities, along with Hillary herself, as Secretary of State.

On Apr. 17, 1995, Bill Clinton’s national security confidante, Professor James P. Chandler, drafted Executive Order No. 12958—Classified National Security Information. Successive Presidents cite back to this order in dozens of related orders, so it governs Hillary Clinton’s current email server conduct. Section 6.1(b) authorizes the Attorney General to interpret the Order. Sec. 5.4(a) established the Secretaries of State & Defense, Attorney General, C.I.A. Director and two Presidential aides as oversight. If the principals are colluding, then accountability is non-existent.

Truly, the foxes are guarding the White House hen house.

ECONOMIC ESPIONAGE ACT—EXECUTIVE ORDER 12356

On Aug. 13, 2015, Hillary Clinton just turned over an empty private email server to the Justice Department. It is a matter of public record that the Justice Department is not impartial since they had oversight of Hillary’s activities, along with Hillary herself, as Secretary of State.

On Apr. 17, 1995, Bill Clinton’s national security confidante, Professor James P. Chandler, drafted Executive Order No. 12958—Classified National Security Information. Successive Presidents cite back to this order in dozens of related orders, so it governs Hillary Clinton’s current email server conduct. Section 6.1(b) authorizes the Attorney General to interpret the Order. Sec. 5.4(a) established the Secretaries of State & Defense, Attorney General, C.I.A. Director and two Presidential aides as oversight. If the principals are colluding, then accountability is non-existent.

Truly, the foxes are guarding the White House hen house.

ECONOMIC ESPIONAGE ACT—EXECUTIVE ORDER 12356

On Aug. 13, 2015, Hillary Clinton just turned over an empty private email server to the Justice Department. It is a matter of public record that the Justice Department is not impartial since they had oversight of Hillary’s activities, along with Hillary herself, as Secretary of State.

On Apr. 17, 1995, Bill Clinton’s national security confidante, Professor James P. Chandler, drafted Executive Order No. 12958—Classified National Security Information. Successive Presidents cite back to this order in dozens of related orders, so it governs Hillary Clinton’s current email server conduct. Section 6.1(b) authorizes the Attorney General to interpret the Order. Sec. 5.4(a) established the Secretaries of State & Defense, Attorney General, C.I.A. Director and two Presidential aides as oversight. If the principals are colluding, then accountability is non-existent.

Truly, the foxes are guarding the White House hen house.
WHITE HOUSE INTELLIGENCE AGENCY (W.H.I.A.)

For this article we'll call this super agency the WHITE HOUSE INTELLIGENCE AGENCY (W.H.I.A.).

W.H.I.A. makes its own rules, gets stealth funding from other agencies, classifies and declassifies its own secrets, co-opts, protects (and sometimes threatens) private industry cronies. W.H.I.A. is accountable only to the President—not Congress or the Courts. In fact, the Courts and the Patent Office tucked tail long ago.

W.H.I.A. operates totally outside Constitutional checks and balances. In reality, W.H.I.A. seems to answer only to designated “critical infrastructure partners” in Wall Street and Silicon Valley.

C.I.A., NSA and FBI REPORT TO W.H.I.A.

Until this new research emerged, AFI investigators had concluded that an out-of-control C.I.A. was the agency that was scrambling our republican governmental processes. However, the last three American presidents have each used W.H.I.A. as their private White House intelligence operation.

W.H.I.A. MAKES NIXON’S PLUMBERS LOOK LIKE SCHOOL BOYS

Richard Nixon resigned over a bungled third rate burglary of the Democratic National Headquarters at the Watergate apartment complex in Washington, D.C. By contrast, Bill Clinton, George Bush and Barack Obama have each used W.H.I.A. to get what they wanted. Nixon’s Plumbers look like school boys by comparison.

BILL CLINTON used these orders to invoke national security over the Monica Lewinsky scandal. He alleged that Monica worked for Israeli intelligence and that Bill was working her for counterintelligence. Who could prove him wrong since W.H.I.A. operates under the unilateral control of the President? Since W.H.I.A. never received Congressional authorization, no normal due process accountability structures exist.

GEORGE BUSH used W.H.I.A. to justify the second Iraq war, including the lies about weapons of mass destruction. It was on George’s watch that W.H.I.A. stole Leader Technologies’ social networking invention. The theft was led by W.H.I.A. progenitor, Professor James P. Chandler—Bill & Hillary’s mentor and Leader’s attorney. W.H.I.A. turned Leader’s invention into a spy-state surveillance platform by luring users, including children. Facebook is just one of their many social creations.

BARACK OBAMA has used W.H.I.A. to fool Saul Alinsky’s “Useful Idiot” masses into electing him, funding his campaigns and stonewalling efforts to get information from this Administration—the “most transparent administration in history.”

NOW, HILLARY CLINTON relies on W.H.I.A. executive orders to justify her lies to Congress about Benghazi, her email servers and The Clinton Foundation, by its various names*

* Clinton Economic Opportunity Initiative, Clinton Health Access Initiative, Alliance for a Healthier Generation, Clinton Global Initiative, Clinton Climate Initiative, Clinton Development Initiative, Clinton-Giustra Enterprise Partnership Initiative, Clinton-Giustra Enterprise Partnership (Canada), Clinton Foundation in Haiti, Clinton Climate Initiative, Clinton Development Initiative, Clinton Health Matters Initiative, No Ceilings, The Full Participation Project, Too Small to Fail, and The Bill, Hillary and Chelsea Clinton Foundation See Tan, S., Hamburger, T., Helderman, R. (Jun 02, 2015) [PDF] How the Clinton Foundation is organized The Washington Post

THE CLINTONS FRONT FOR W.H.I.A.'S GLOBAL AGENDA

The many Clinton foundations are very evidently fronting organizing activity for W.H.I.A. Their rhetoric is awash in Orwellian double-speak about national security, privacy, economic well-being and security. But, the fact is that their efforts undermine American sovereignty, collect Orwellian “dark profiles” on every citizen, and impoverish the economy.

W.H.I.A. GODFATHER JAMES P. CHANDLER WAS APPOINTED TO NIAC JUST TWO DAYS BEFORE BILL CLINTON LEFT THE WHITE HOUSE

On Jan. 18, 2001, two days before his departure, Bill Clinton appointed Leader Technologies’ patent attorney, James P. Chandler—Bill & Hillary’s mentor and Leader’s attorney. W.H.I.A. makes Nixon’s Plumbers look like school boys by comparison.

1. HOW PATENT JUDGES GROW RICH ON THE BACKS OF AMERICAN INVENTORS
   Patent Office filings are shuffled out the USPTO backdoor to crony lawyers, banks and deep-pocket clients.

2. WAS CHIEF JUSTICE ROBERTS BLACKMAILED into supporting Obamacare by his ethical compromises in Leader v. Facebook?

3. JUSTICE ROBERTS MENTORED Facebook Gibson Dunn LLP attorneys.

4. JUSTICE ROBERTS HOLDS substantial Facebook financial interests.

5. JUDGE LEONARD STARK FAILED to disclose his Facebook financial interests and his reliance on Facebook’s Cooley Godward LLP attorneys for his appointment.

BARACK OBAMA'S DARK POOLS OF CORRUPTION

Click to enlarge

STOP FACEBOOK PROPERTY THEFT

We see. We “like.” We steal. www.fbcoverup.com

WILL HUMANKIND EVER LEARN? Facebook’s Orwellian doublespeak about property and privacy (theft) merely repeats the eventual dehumanization of the individual under Mao’s Red Star, Stalin’s SOVIET Hammer & Cycle and Hitler’s NAZI Swastika. Respect for the inalienable rights of each individual is a bedrock value of democracy. The members of the Facebook Cabal abuse this principle every opportunity. They evidently believe that they deserve special privileges and are willing to lie, cheat and steal in order to treat themselves to these privileges.

ASK CONGRESS: PASS THE

http://americans4innovation.blogspot.com/2015/08/hillary-bill-shill-for-secret-intelligence-agency-car tel.html
Chandler, to his NATIONAL INFRASTRUCTURE ASSURANCE COUNCIL (NIAC). NIAC members read like a Who’s Who of IBM’s Eclipse Foundation.

For Bill, this last Executive Order was merely a stepping stone into his Pied Piper work for his foundations where he has pursued the spy-state agenda with a vengeance. It was only the end of Chapter 1 of the takeover by a totalitarian left.

On Mar. 14, 2001, Chandler pushed through sweeping Judicial Conference changes to the mutual fund ethics disclosure guidelines. These changes opened the door to widespread abuse by judges and judicial employees who now hide their deep-pocket investments behind mutual fund veils. Then for example, even if JPMorgan is a litigant in the case, the judge who holds JPMorgan stocks in various mutual funds will preside over the case while silently making decisions favorable to JPMorgan (and his stock portfolio). See Hijack of the Cyberworld Timeline.


On Mar. 21, 2001, social networking inventor Michael McKibben, Leader Technologies, presented a plan to Chandler and Battelle Memorial Institute to implement an innovation at Harvard with IBM. It was called THE UNIVERSITY INITIATIVE. The Chandler and the Cartel stole Leader’s plan, which became the spy-state platform Facebook.

On Nov. 29, 2001, ten months later, Chandler and IBM formed another foundation, THE ECLIPSE FOUNDATION, to hijack Leaders’ social networking invention.

In 2009, IBM’s inside counsel, DAVID J. KAPPOS, was appointed by Obama to run the Patent Office in 2009. ERIC H. HOLDER, JR. was appointed as Attorney General. Both men are Chandler underudies.

OBAMA FOLLOWS ALONG IN LOCKSTEP

On Feb. 13, 2015, just six months ago, Barack Obama doubled-down on W.H.I.A. with Executive Order No. 13691, “Promoting Private Sector Cybersecurity Information Sharing.” Both Holder and Kappos have moved to Cartel jobs since leaving Obama, as have many others in this White House.

EXECUTIVE BRANCH STONEWALLING EMANATES FROM W.H.I.A.

Obama’s latest order is just the latest in a string of related orders he has issued since 2009. These orders have given the Attorney General (Eric H. Holder, Jr.) almost dictatorial powers over W.H.I.A.

Among these W.H.I.A. orders were authorizations to issue security clearances for commercial vendors, to classify and declassify documents by their own rules (Hillary’s email server was not classified if she said so), and invoke executive privilege on information requested by subpoena and FOIA requests. W.H.I.A. appears to be the authority being used by the White House to stonewall Congress, Inspectors General and FOIA requests.
ORDERS ESTABLISHING W.H.I.A. ARE A RAT’S NEST OF LEGAL Gobbledygook

The Executive Orders are chock full of bureaucratic legalese and gobbledygook. No human can decipher the nested references from one order to another. Consequently, they are an unscrupulous lawyer’s playground, which appears to be by design.

For example (now stay with us):

---

Sec. 6. General Provisions. (a) This order does not change the requirements of Executive Orders 13526, 12869, 15467, or 13289, as amended, and their successor orders and directives.

(b) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.); the Secretary of Defense under Executive Order 12899, as amended; the Director of the Information Security Oversight Office under Executive Order 13356 and Executive Order 12824, as amended; the Attorney General under title 18, United States Code, and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 5101 et seq.); the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic and Consular Independence and Security Act of 1986; or the Director of National Intelligence under the National Security Act of 1947, as amended, Executive Order 12333, as amended, Executive Order 12906, as amended, Executive Order 13467, and Executive Order 13326.

---

Got it? Exactly. Only the mother of a monster could love what you just read.

A STUPID SMART LAW PROFESSOR CREATED W.H.I.A.

What would possess a Washington, D.C. insider to conceive of such a scheme and think he could get away with it? Only a well-healed national security law professor like James P. Chandler could keep an operation like this together and secret through three presidents.

Chandler is intelligent and cunning. He appears to be almost single handedly responsible for much of the racial agenda emerging from the White House. His oversized intellect keeps him ahead of most people. In Chandler’s mind, payback would indeed be a bitch, we believe.

Chandler was a Harvard Law professor. Barack Obama appears to be Chandler’s Manchurian candidate. The same is true for two other Chandler protégés: Eric H. Holder, Jr. as Attorney General and IBM’s David J. Kappos as Patent Office Director.

This doesn’t even count Lawrence “Larry” Summers who was president at Harvard when Chandler, Fenwick & West LLP and James W. Breyer, Accel Partners LLP, came to him with the Leader Technologies’ University Initiative, albeit repackaged as Facebook.

Summers hired his former Harvard student, Sheryl K. Sandberg, and fledgling Russian banker Yuri Milner as his researchers when he became Chief

---

JAMES P. CHANDLER’S SELLOUT OF HIS CLIENT, LEADER TECHNOLOGIES, INC. (WHISTLEBLOWER REVELATIONS)

---

GIBSON DUNN LLP exposed as one of the most corrupt law firms in America

Investigative Reporter Julia Davis investigates Facebook’s Leader v. Facebook attorney Gibson Dunn LLP. She credits this firm with the reason why not a single Wall Street banker has gone to jail since 2008. Click here to read her article “Everybody hates whistleblowers.” Examiner.com, Apr. 10, 2012. Here’s an excerpt:

-Skillful manipulation of the firm’s extensive media connections allows Gibson Dunn to promote their causes, while simultaneously smear their opponents and silencing embarrassing news coverage.”

This statement followed right after Davis cited Facebook’s chief inside counsel in the Leader v. Facebook case, Theodore Ullyot, who appears to have helped lead the Leader
Economist at the World Bank in 1992. See **Summers-Sandberg-Milner Timeline**. Does anyone think it is coincidence that Sandberg is Facebook’s chief operating officer and Milner’s Moscow, Russia investments drove Facebook’s pre-IPO valuation to $100 million by 2012? Instead of doing the right thing, Breyer deployed his venture capital influence at the National Venture Capital Association (NVCA) to carve up and fund exploitation of Leader’s invention into market-by-market pieces. Facebook for universities, LinkedIn for professionals, Instagram for pictures, Twitter for messages, Palantir for spy-state surveillance, Athenahealth for medical offices. . . you get the picture.

It was a feeding frenzy. That’s when 19-year old Mark Zuckerberg agreed to lie for them and be their Harvard front man in 2003.

Ethically, Chandler evidently prefers patent theft, subversiveness, deception and skin color over legal acumen, morals and common decency. . . all for the common good and national security, of course.

Chandler also appears to be the person within the White House who orchestrates the FOIA stonewalling that was recently revealed to the House Oversight Committee.

Washington, D.C. court records show that Chandler has been involved in at least three civil rights cases, one involving himself, and two his son. All three cases were complaints involving police. His case was settled and his son’s were dismissed. This focus on race cases may help explain why the flames in Ferguson are fueled by well-financed outsiders. Chandler appears to have his largesse stashed in the Cayman Islands in James LLC, among others.

**CHANDLER DEMANDS PUBLIC ADMIRATION**

Chandler’s recently leaked stenographer notes from 2002 revealed a Trump-sized self-promoter when he told Montgomery County, Maryland officials: “We do valuable work for our country and it is important for that to be understood and acknowledged.” See Fig. 5.

**CHANDLER FORMED THE ECLIPSE FOUNDATION IN 2001 WITH IBM, HIS GO TO W.H.I.A. TECHNOLOGY PROVIDER**

On Nov. 29, 2001, IBM and Chandler formed The Eclipse Foundation, ostensibly to become a repository for “contributed” IBM Open Source software, an oxymoron in itself.

IBM is the largest holder of patents on the planet. IBM does not do Open Source. What IBM did was receive was Leader’s source code from Chandler, then IBM claimed Leader’s invention as their own. In short, the Eclipse IDE (interface development environment) is Leader’s invention.

The innovative elements of the Eclipse IDE were not IBM’s and Chandler’s property to give away.

**TRANSCRIPT of Kelley Clements’ stenographer’s notes above:**

We have no reluctance to share info, with the County - DO NOT GO PUBLIC w/ this

We do valuable work for our country and it is important for that to be understood and acknowledged

Doug Duncan is aware [Montgomery County, Maryland, Executive]

NIPLI [Chandler’s National Intellectual Property Law Institute] to define space spec
- what we need
- what we don’t need

IBM Incorporating Members
Business Model - different from current business model
- consider some approach to partnering w/ IBM

**SPEND THE ECLIPSE CASH AND RECRUIT IBM PARTNERS WITHOUT DISCLOSING HIS CONFLICTS OF INTEREST TO HIS OTHER CLIENT, LEADER TECHNOLOGIES, INC.**

**GRAPHIC: CHANDLER NOTES**

**FIG. 8—IBM ECLIPSE FOUNDATION MEMBERS, PAGE 1, PREPARED AS OF SEPT. 09, 2008 AND REPORTED TO THE BOARD OF DIRECTORS ON SEPT. 17, 2008. CLICK HERE FOR IMAGE OF PAGE 2.**


**Massive Washington Corruption Exposed by Leader v. Facebook**

Bi-partisan citizen group appeals to Congress to restore property

**Confiscated by widespread federal corruption incl. interference by Nancy Pelosi...**

**Healthcare.gov has exposed Washington’s ethical disease**

Undisclosed conflicts of interest—on a massive scale—are choking Washington

**Boycott NCAA March Madness? Copyright-Gate**

Constitutional rights advocates demand that NCAA stop its copyright infringement in social media; ask Congress to preserve Zuckerberg’s...
BILL & HILLARY (AND BARACK) ARE PIED PIPERS FOR THE ECLIPSE FOUNDATION, FACEBOOK & W.H.I.A. AGENDA FOR GLOBAL DOMINATION—NO WONDER THEY RAISED $2 BILLION (WITH A "B") FOR THEIR FOUNDATIONS!

An analysis of Hillary Clinton's 2009, 2010, 2011 and 2014 financial disclosures reveal a correlation between Eclipse Foundation members and Bill's speaking 126 speaking engagements over a 40-month period. 22 companies are direct members of Eclipse, while dozens others are financiers and customers of those Eclipse vendors that include Microsoft, Cisco, Salesforce.com, DocuSign, Verisign, CareerBuilder, Visa, McAfee, Deloitte & Touche, Oracle, UBS, AT&T, SAP, Deutsche Bank, Castlight Health, eBay, Qualcomm, Xerox, GE, Vanguard, Bank of America/Merrill Lynch, and Barclays. Over half of these companies are Facebook underwriters and beneficiaries. Over half of these companies are Facebook underwriters and beneficiaries. See The Washington Post. [Return shortly to this post for a link to a spreadsheet being prepared to be linked here.]

HILLARY'S FINANCIAL DISCLOSURES CONTAIN CRIMINAL OMISSIONS

Prior to Hillary’s appointment as Secretary of State in 2009, she submitted a financial disclosure on Jan. 05, 2009. However, that 2008 report has disappeared from the Office of Government Ethics website.

AFI obtained a copy nonetheless from OpenSecrets.org. Click here for Hillary Clinton's 2008 financial disclosure. Why did the White House block public access to Hillary’s financial report, which had been public? It is evidently because she totally neglected to disclose her financial interests in her foundations.

Hillary failed to disclose her Clinton Foundation and PAC activities in any manner that an experienced attorney like her knows she should. For example, here is the extent of her now concealed 2008 disclosure:

Only disclosure about her foundations in her 2008 financial disclosure. The disclosure omits the tens of millions accumulated to her benefit by Bill Clinton’s speaking fees, which averaged $117,000 per event. Such nondisclosure is illegal, if it was a knowing omission intended to deceive the public.

Hillary did not disclose a single dollar of financial interest associated with her foundations or PACs. However, according to The Washington Post, Bill and Hillary have raised over $2 billion for the foundations. Propriety dictates that such enormous cash flow must be disclosed. Failure to disclose is not inadvertent, but obviously willful, and therefore criminal.

Bill Clinton has made over $104.9 million in speeches since leaving office in 2001 to promote The Eclipse Foundation and W.H.I.A, also according to The Washington Post. Hillary disclosed nothing about the financial’s of her foundations in 2008. Perhaps this explains why the White House has removed that report from the Office of Government Ethics (OGE) website.

Bookmark: #hillary-clinton-financial-disclosures

NEW: CLINTON, HILLARY R., 2000–2015 FINANCIAL DISCLOSURES

Total Speaking Fees, All Events (2000-2014): PDF | Excel Spreadsheet (*.xlsx)
Total IBM Eclipse Foundation Speaking Fees (2000-2014): PDF | Excel Spreadsheet (*.xlsx)

FIG. 10—HILLARY R. CLINTON’S FINANCIAL DISCLOSURES (2000-2015)

CHRISTINA M. CHEN, HILLARY’S CHIEF OF STAFF, IS EQUALLY DECEPTIVE

The financial disclosure for Christina M. Tchen, Hillary’s chief of staff, has also disappeared from the OGE website. However, AFI was able to obtain a copy from a whistleblower. Click here for Christian M. Tchen 2008 Financial Disclosure.

http://americans4innovation.blogspot.com/2015/08/hillary-bill-shill-for-secret.html
Tchen apparently couldn’t get a good scanner on her $2.2 million Skadden Arps LLP annual Chicago lawyer salary before coming to work at the White House. Here is her disclosure in regular and zoomed modes:

Tina M. Tchen Disclosure @ 100% (full size) Magnification (illegible):

Tina M. Tchen Disclosure @ 200% (2x) Magnification (still almost unreadable):

An AFI researcher studied the Tchen’s disclosure until her eyes bled. (Eyes folks, eyes [inside joke for those following Donald Trump’s dust up with FoxNews’ Megyn Kelly].) She determined that Tchen worked for Skadden Arps LLP. Skadden Arps currently represents JPMorgan in Dr. Lakshmi Arunachalam’s patent infringement battle. Arunachalam-Pi-Net v. JPMorgan. Skadden has been proven to lie for JPMorgan in every court filing and in front of the judge.

One judge in that case, Richard G. Andrews, actually admitted on the record that he holds JPMorgan stock, yet still refused to disqualify himself, citing the “safe harbor rule,” which is not a rule or even and opinion. The Advisory where it appears (p. 200) refers to it merely as a “concept” with four pages of exceptions. Earlier in the advisory, in Section 20 on page 24, it says that even one share of stock held by a spouse requires a judge to recuse! And, yet, these corrupt judges have created their excuse and they’re sticking too it. Tchen’s association with the crooked Skadden Arps law firm speaks volumes about her ethical standards brought to Hillary and The White House.

The judicial misconduct has deteriorated from there, replete with two of the three judges on the Federal Circuit appeal panel, Judges Alan D. Lourie and Kimberly A. Moore, holding Facebook stock that they did not disclose to the litigants, and later tried to excuse through a quick motion slipped in at the last minute by the Clerk of Court, Jan Horbaly, and his close friends at The Federal Circuit Bar Association. (The DC Bar subsequently revealed that Mr. Horbaly is not licensed to practice law in Washington D.C.)

The judges ignored shocking new evidence that Mark Zuckerberg withheld 28 hard drives of 2003-2004 evidence from Leader Technologies that could prove actual theft (and therefore claims even more serious than infringement). In addition, Facebook’s appeal attorney, Thomas G. Hungar of Gibson Dunn LLP, has close personal ties to just about every judicial player in this story. The misconduct appears to reach into the U.S. Patent Office through abuse of the reexamination process by Facebook. We will stay focused on Leader v. Facebook until justice is served, but we also welcome news and analysis of intellectual property abuse in other cases as well.

WELCOME TO DONNA KLINE NOW! READERS!

AFI has been supporting Donna and is now picking up the main Leader v. Facebook coverage (she will continue coverage as well).

Anonymous Posts Are Welcomed! Blogger has more posting constraints than Donna’s WordPress, but we will continue to welcome anonymous posts. Simply send us an email at amer4innov@gmail.com with your post. Once the moderator verifies that your email address is real, your comment will be posted using your real name or handle, whatever you wish, like John Smith or Tex.

Click here to view a complete Donna Kline Now! posts archive.
Tchen disclosed that her salary at Skadden Arps in Chicago was $2.2 million per year. She also disclosed that she had up to $8,723,000 in financial holdings.

Hillary's chief of staff, a seasoned attorney, filed an illegible financial disclosure by accident? Um, uh huh.

**CHANDLER’S GREED, ARROGANCE & NARCISSISM**

In conclusion, Bill & Hillary work for the W.H.I.A. Eclipse Cartel. This Cartel stole Leader Technologies’ social networking patent, gave it to IBM, Eclipse and Facebook, used it get Barack Obama funded and elected, twice. Obama's social networking cronies have been raping and pillaging ever since.

The NSA has exploited the user data of the world's children, then lied about it to Congress. It took a brave whistleblower named Edward Snowden to reveal the truth about this illegal activity.

It took another brave whistleblower, HSBC Swiss Hervé Falciani, to reveal that this Cartel is cavorting with drug and arms dealers in offshore banks to hide their illegal activity.

NEW: It took the bravery of Julian Assange and WikiLeaks to blow the whistle on Austin-based Stratfor by releasing five million emails from this C.I.A. disinformation front. These documents validated that Facebook was founded and funded by the C.I.A. and this same group of technology providers and banks cavort with the arms and drug leaders exposed by Falciani. See previous post: Facebook started by C.I.A. as spy-state tool.

The current bastardization of Leader Technologies’ social networking invention by the Eclipse Foundation cartel started when a previously well-respected law professor, James P. Chandler, who ignored his ethical oath, betrayed his client, then sold his soul for thirty pieces of silver.

Like Narcissus, Professor Chandler's admiration of himself will likely be his undoing. He does not appear to be as smart as advertised, in our opinion.

Whistleblowers we await your additional revelations! If you wait too long, your information will lose negotiating value.

* * *

**NEW, AUG. 15, 2015**

Judge Leonard P. Stark, U.S. District Court of Delaware, trial Judge in Leader Techs, Inc. v. Facebook, Inc., 770 F. Supp. 2d 686 (D.Del. 2011). Judge Stark heard his jury foreman admit that the jury made the on-sale bar decision without any evidence other than speculation, and yet he supported that verdict anyway. Just months before trial, Judge Stark allowed Facebook to add the on-sale bar claim after the close of all fact
Between 2001 and 2015, Bill & Hillary Clinton disclosed in public financial disclosures that they have been paid $15.5 million from 75 events ($206,000 average) for IBM Eclipse Foundation members. Overall, they have been paid $117 million from 593 events ($117,000 average). The Eclipse IDE (Interface Development Environment) is based on the inventions of Columbus, Ohio innovator, Leader Technologies, that were stolen and shuffled to IBM and Eclipse for exploitation by the C.I.A., NSA and W.H.I.A. in general by James P. Chandler, who in 2001 was intellectual property patent counsel to both IBM and Leader Technologies. Click here for Hillary & Bill Clinton 2001-2015 IBM Eclipse Foundation Member Speaking Fee Summaries: Excel Spreadsheet (*.xlsx). Click here for a PDF Version.


Notice: This post may contain opinion. As with all opinion, it should not be relied upon without independent verification. Think for yourself.

COMMENT

Click 'N comments:' on the line just below this instruction to comment on this post. Alternatively, send an email with your comment to amer4innov@gmail.com and we’ll post it for you. We welcome and encourage anonymous comments, especially from whistleblowers.

Posted by K. Craine at 8:36 PM

3 comments:

K. Craine August 12, 2015 at 12:48 PM

Email comment by TEX:

My gal Friday, Flavia, bounced in the office this morning and said, “ they will never prosecute Hillary, she knows too much. She will squeal like a little pig . . . . she has something nefarious on everyone in the cartel.” . . . Bingo !! But they (the DOJ) have to play the game, nonetheless. It will be a quick DOJ review of her emails, and , wahla , a proclamion of innocence. The big danger for the cartel is the FBI. They seem to be
outside the control of Chandler, Obama, Clinton, the DOJ, et al. It is clear that the Obama’s, especially man/woman Michelle, do not care for Hillary. If the FBI pursues Hillary’s obvious criminality, she will sing like a full throated warbler. You think the Donald can get ugly, you ain’t seen nothing yet. This big ball of yarn has a loose end, and Mr Gowdy and the boys are going to pull that string into hell for the Clintons. I can’t get this smile off of my face........

Have a great day, TEX

PS. Flavia didn’t say nefarious. I made that up. She used a potty mouth word. She thinks nefarious is a ride at the Fair.

K. Craine  August 15, 2015 at 7:40 PM

AT&T Helped U.S. Spy on Internet on a Vast Scale


According to the map just published above:

http://americans4innovation.blogspot.com/2015/08/hillary-bill-shill-for-secret.html

Bill Clinton was paid $225,000 by AT&T to speak at an event in Tucson on Nov. 20, 2014. Judging from the NSA documents cited in the Times article, Bill was a prime mover in the current global snooping. Also, we noted in the slides that the NSA relies heavily on that 2008 FISA amendment (FAA) that Chandler pushed through weeks after Obama was elected in 2008 and six weeks before Eric Holder was appointed in earlier 2009. That amendment gave Holder almost dictatorial powers. AFI has written about that Amendment at:

http://americans4innovation.blogspot.com/2014/07/eric-holder-exploits-secret-fisa-laws.html

K. Craine  August 18, 2015 at 10:09 AM

Given the central role of the Secretary of State in Obama’s secret national security infrastructure, created by Executive Orders, Presidential Policy Directives (PPDs) and Homeland Security Policy Directives (HSPDs), it is inconceivable that Hillary Clinton did not receive and respond to secret and top secret communications in her 60,000 emails. That is, unless Chelsea’s wedding rivaled organizing for the Olympics!

For example, here is just one Top Secret PPD-20 leaked by Edward Snowden pulling back the covers on Obama’s spy state:

U.S. Cyber Operations Policy, PPD-20 TOP SECRET:


http://www.washingtonexaminer.com/state-dept-uncovers-17000-missing-emails/article/2570331

See disclosure of substantial holdings in Facebook and Facebook-related stocks. Judge Moore failed to follow the long-held precedent for testing on-sale bar evidence in Pfaff v. Wells Electronics, Inc.—an evident and intentional omission coming from a former patent law professor. After debunking all of Facebook’s evidence on appeal, Judge Moore created new argument in the secrecy of chambers to support Facebook and prevent the on-sale bar verdict from being overturned—a clear breach of constitutional due process.

Judge Evan J. Wallach, U.S. Court of Appeals for the Federal Circuit, member of the three-judge panel in Leader Techs v. Facebook, Inc., 678 F.3d 1300 (Fed. Cir. 2012). Judge Wallach is not a patent attorney. This begs the question as to why a judge with no knowledge of patent law was assigned to the case. Would anyone ask a dentist to perform brain surgery? The Federal Circuit was specially formed to appoint patent-knowledgeable judges to patent cases. There is no evidence so far in the judicial disclosures that Judge Wallach holds stock in Facebook, although when he was asked on a motion to disclose potential Facebook holdings and other conflicts of interest, he refused along with the other judges. See Motion to Disclose Conflicts of Interest. Judge Wallach continued in silence even after Clerk of Court Horbaly refused to provide him with Dr. Lakshmi Arunachalam’s motions (according to his Federal Circuit staffer Valeri White), and yet the Clerk signed an order regarding that motion on Judge Wallach’s behalf. See a full analysis of these events at Donna Kline Now! Judge Wallach also failed to police his court’s violation of Leader’s Fifth and 14th Amendment constitutional right to due process when he participated in the fabrication of new arguments and evidence for Facebook in the secrecy of Judge’s chambers after he had just invalidated Facebook’s sole remaining item of evidence (using disbelieved testimony as ostensibly evidence of an opposite). Judge Wallach also
COVERT OPERATION TO SPY ON AMERICANS

Eclipse = Cover up the U.S. Constitution

1. Leader Technologies, Inc.
The Eclipse Foundation
C.I.A.

Leader hired Chandler & Fenwick as custodians to protect their inventions

2. Strategy
Chandler & Fenwick secretly fed Leader’s invention to the CIA via IBM and Eclipse

3. Disinfection (pollute facts)
• Stratfor (ABC, NBC, CBS, CNN, CNBC, MSNBC, FOX, Comcast, BBC)

• David J. Kappos
• Patent Office Judges & Examiners
• Federal Circuit

4. Funding
• C.I.A. – In-Q-Tel
• JPMorgan
• Morgan Stanley
• UBS
• Citigroup
• Wells Fargo
• Barclays
• Goldman Sachs
• T. Rowe Price
• Vanguard
• BlackRock
• Bank of America
• Fidelity
• TIAA CREF
• Baillie Gifford
• HSBC

5. Legal Hitmen
• Gibson Dunn LLP
• Cooley Godward LLP
• Fenwick & West LLP
• Latham & Watkins LLP
• Orrick Herrington LLP
• White & Case LLP
• Weil Gotshal LLP
• Perkins Coie LLP
• Blank Rome LLP
• Fed. Cir. Bar Assoc.
• DC Bar Assoc.
• Harvard Law
• Stanford Law
• Yale Law

6. Technology
• IBM
• Microsoft
• Eclipse Foundation
• Eclipse IDE
• NSA PRISM:

09/11/07 Microsoft
03/12/08 Yahoo
01/14/09 Google
06/03/09 Facebook
12/07/09 PalTalk
09/24/10 YouTube
02/06/11 Skype
03/31/11 AOL
10/01/12 Apple (one year after Steve Jobs died)

7. Fronts
• Facebook
• LinkedIn
• Instagram
• Common Core / MOOC
• Pinterest
• Groupon
• Zynga
• Mail.ru (Russia)
• Eurotech, Ltd.
• Eurotech SpA (Italy)
• The White Oak Group
• James LLC (Caymans)
• Accel Partners LLP
• IDG-Accel (China)
• IDG Capital (China)
• Baidu (China)
• Wininchina, Inc.
• Microsoft
• athenahealth/Castlight Health
• IBM
• Lenovo (China)
• Tsinghua University (China)
• Soros Fund Management LLC

8. Corruption
• Eric H. Holder, Jr.
• John G. Roberts, Jr.
• Justice Department
• Judicial Conference
• Judiciary Committees
• Federal Judiciary
• FISA Court
• America Invents Act
• HealthCare.gov
• Fast & Furious / AP snooping
• IRS targeting
• Net Neutrality
• Trans-Pacific Partnership (TPP)
• Iran Deal

• “Safe harbor concept” used as ethics excuse for carte blanche judicial financial nondisclosure

• False Statement Accountability Act of 1996 (these people may lie to courts, Congress and The People without liability)

What other than capitulation to CIA threats could have gotten these competitors to fall in line?

Is the solar eclipse symbol of Islam just a coincidence?

Qur’anic Scholar: “If a Muslim feels threatened, he is permitted to lie to ‘people of the book’ (Infidels: Christians, Jews, Westerners).” See Q. 98:6, 3:51, 3:28. Does this sound like an Administration we know?

Notice: This document may contain opinion that should not be relied upon without independent verification. Think for yourself.

Rev. Jul. 18, 2015
formation that legitimately needs to be guarded in the interests of national security. In issuing this order, I am seeking to bring the system for classifying, safeguarding, and declassifying national security information into line with our vision of American democracy in the post-Cold War world.

This order strikes an appropriate balance. On the one hand, it will sharply reduce the permitted level of secrecy within our Government, making available to the American people and posterity most documents of permanent historical value that were maintained in secrecy until now. On the other, the order enables us to safeguard the information that we must hold in confidence to protect our Nation and our citizens. We must continue to protect information that is critical to the pursuit of our national security interests. There are some categories of information—for example, the war plans we may employ or the identities of clandestine human assets—that must remain protected.

This order also will reduce the sizable costs of secrecy—the tangible costs of needlessly guarding documents and the intangible costs of depriving ourselves of the fullest possible flow of information.

This order establishes many firsts: Classifiers will have to justify what they classify; employees will be encouraged and expected to challenge improper classification and protected from retribution for doing so; and large-scale declassification won't be dependent on the availability of individuals to conduct a line-by-line review. Rather, we will automatically declassify hundreds of millions of pages of information that were classified in the past 50 years.

Similarly, we will no longer tolerate the excesses of the current system. For example, we will resolve doubtful calls about classification in favor of keeping the information unclassified. We will not permit the reclassification of information after it has been declassified and disclosed under proper authority. We will authorize agency heads to balance the public interest in disclosure against the national security interest in making declassification decisions. And, we will no longer presumptively classify certain categories of information, whether or not the specific information otherwise meets the strict standards for classification. At the same time, however, we will maintain every necessary safeguard and procedure to assure that appropriately classified information is fully protected.

Taken together, these reforms will greatly reduce the amount of information that we classify in the first place and the amount that remains classified. Perhaps most important, the reforms will create a classification system that Americans can trust to protect our national security in a reasonable, limited, and cost-effective manner.

In keeping with my goals and commitments, this order was drafted in an unprecedented environment of openness. We held open hearings and benefitted from the recommendations of interested Committees of Congress and nongovernmental organizations, groups, businesses, and individuals. The order I have signed today is stronger because of the advice we received from so many sources. I thank all those who have helped to establish this new system as a model for protecting our national security within the framework of a Government of, by, and for the people.

William J. Clinton

The White House,
April 17, 1995.

Executive Order 12958—Classified National Security Information
April 17, 1995

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation’s progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation’s security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the
national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

**Now, Therefore,** by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Part 1 Original Classification**

**Section 1.1. Definitions.** For purposes of this order:

(a) “National security” means the national defense or foreign relations of the United States.

(b) “Information” means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. “Control” means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) “Classified national security information” (hereafter “classified information”) means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(d) “Foreign Government Information” means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as “Foreign Government Information” under the terms of a predecessor order.

(e) “Classification” means the act or process by which information is determined to be classified information.

(f) “Original classification” means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) “Original classification authority” means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) “Unauthorized disclosure” means a communication or physical transfer of classified information to an unauthorized recipient.

(i) “Agency” means any “Executive agency,” as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

(j) “Senior agency official” means the official designated by the agency head under section 5.6(c) of this order to direct and administer the agency’s program under which information is classified, safeguarded, and declassified.

(k) “Confidential source” means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) “Damage to the national security” means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

**Sec. 1.2. Classification Standards.** (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and

(4) the original classification authority determines that the unauthorized dis-
closure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Sec. 1.3. Classification Levels. (a) Information may be classified at one of the following three levels:

(1) “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.4. Classification Authority. (a) The authority to classify information originally may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; or

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) “Top Secret” original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) “Secret” or “Confidential” original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated “Top Secret” original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear
which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.5. Classification Categories.

Information may not be considered for classification unless it concerns:

(a) military plans, weapons systems, or operations;
(b) foreign government information;
(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
(d) foreign relations or foreign activities of the United States, including confidential sources;
(e) scientific, technological, or economic matters relating to the national security;
(f) United States Government programs for safeguarding nuclear materials or facilities;
(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Sec. 1.6. Duration of Classification. (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

(1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;
(2) reveal information that would assist in the development or use of weapons of mass destruction;
(3) reveal information that would impair the development or use of technology within a United States weapons system;
(4) reveal United States military plans, or national security emergency preparedness plans;
(5) reveal foreign government information;
(6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;
(7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
(8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, “Originating Agency’s Determination Required,” or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.7. Identification and Markings. (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.3 of this order;
(2) the identity, by name or personal identifier and position, of the original classification authority;
(3) the agency and office of origin, if not otherwise evident;
(4) declassification instructions, which shall indicate one of the following:
   (A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or
   (B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or
   (C) the exemption category from declassification, as prescribed in section 1.6(d); and
(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Sec. 1.8. Classification Prohibitions and Limitations. (a) In no case shall information be classified in order to:
   (1) conceal violations of law, inefficiency, or administrative error;
   (2) prevent embarrassment to a person, organization, or agency;
   (3) restrain competition; or
   (4) prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:
   (1) meets the standards for classification under this order; and
(2) is not otherwise revealed in the individual items of information.

As used in this order, “compilation” means an aggregation of pre-existing unclassified items of information.

Sec. 1.9. Classification Challenges. (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

(1) individuals are not subject to retribution for bringing such actions;
(2) an opportunity is provided for review by an impartial official or panel; and
(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

Part 2 Derivative Classification

Sec. 2.1. Definitions. For purposes of this order: (a) “Derivative classification” means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) “Classification guidance” means any instruction or source that prescribes the classification of specific information.

(c) “Classification guide” means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) “Source document” means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) “Multiple sources” means two or more source documents, classification guides, or a combination of both.

Sec. 2.2. Use of Derivative Classification. (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and
(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and
(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.3. Classification Guides. (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and
(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.
Part 3 Declassification and Downgrading

Sec. 3.1. Definitions. For purposes of this order: (a) “Declassification” means the authorized change in the status of information from classified information to unclassified information.

(b) “Automatic declassification” means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or
(2) the expiration of a maximum time frame for duration of classification established under this order.

(c) “Declassification authority” means:

(1) the official who authorized the original classification, if that official is still serving in the same position;
(2) the originator’s current successor in function;
(3) a supervisory official of either; or
(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) “Mandatory declassification review” means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) “Systematic declassification review” means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States (“Archivist”) to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) “Declassification guide” means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) “Downgrading” means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) “File series” means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Sec. 3.2. Authority for Declassification. (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or
(2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.3. Transferred Information. (a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for
which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

Sec. 3.4. Automatic Declassification. (a) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

(1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;

(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

(9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption
categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

1. a description of the file series;
2. an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and
3. except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

1. a description of the information;
2. an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and
3. except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

Sec. 3.5. Systematic Declassification Review. (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

1. recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or
2. the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the
Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.6. Mandatory Declassification Review. (a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;
(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and
(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester’s appeal rights.

(b) Information originated by:

(1) the incumbent President;
(2) the incumbent President’s White House Staff;
(3) committees, commissions, or boards appointed by the incumbent President; or
(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist’s decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency
decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Sec. 3.7. Processing Requests and Reviews. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order.

In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.8. Declassification Database. (a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Governmentwide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

Part 4 Safeguarding

Sec. 4.1. Definitions. For purposes of this order: (a) “Safeguarding” means measures and controls that are prescribed to protect classified information.

(b) “Access” means the ability or opportunity to gain knowledge of classified information.

(c) “Need-to-know” means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) “Automated information system” means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) “Integrity” means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) “Network” means a system of two or more computers that can exchange data or information.

(g) “Telecommunications” means the preparation, transmission, or communication of information by electronic means.

(h) “Special access program” means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Sec. 4.2. General Restrictions on Access.

(a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head’s designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.
(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

1. prevent access by unauthorized persons; and
2. ensure the integrity of the information.

(f) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States “Confidential” information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Sec. 4.3. Distribution Controls. (a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.4. Special Access Programs. (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

1. the vulnerability of, or threat to, specific information is exceptional; and
2. the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or
3. the program is required by statute.

(b) Requirements and Limitations. (1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably
small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order. Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency’s special access programs.

(c) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency’s jurisdiction. These officials shall terminate any special access programs that do not clearly meet the requirements of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.5. Access by Historical Researchers and Former Presidential Appointees. (a) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects; or
(2) previously have occupied policymaking positions to which they were appointed by the President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of national security;
(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and
(3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

Part 5 Implementation and Review

Sec. 5.1. Definitions. For purposes of this order: (a) “Self-inspection” means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) “Violation” means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or
(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(c) “Infraction” means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a “violation,” as defined above.
Sec. 5.2. Program Direction. (a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

(1) classification and marking principles;
(2) agency security education and training programs;
(3) agency self-inspection programs; and
(4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

Sec. 5.3. Information Security Oversight Office. (a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;
(2) oversee agency actions to ensure compliance with this order and its implementing directives;
(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;
(4) have the authority to conduct on-site reviews of each agency’s program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;
(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;
(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;
(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;
(8) report at least annually to the President on the implementation of this order; and
(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.4. Interagency Security Classification Appeals Panel. (a) Establishment and Administration.

(1) There is established an Interagency Security Classification Appeals Panel
The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members. (2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above. (3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel. (4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel’s functions. (5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner. (6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel’s activities. (b) Functions. The Panel shall: (1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order; (2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and (3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order. (c) Rules and Procedures. The Panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which: (1) the appellant has exhausted his or her administrative remedies within the responsible agency; (2) there is no current action pending on the issue within the federal courts; and (3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years. (d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel. (e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President. Sec. 5.5. Information Security Policy Advisory Council. (a) Establishment. There is established an Information Security Policy Advisory Council (“Council”). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons who have demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. 2. (b) Functions. The Council shall: (1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this order or its implementing directives, including recommended changes to those policies;
(2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and
(3) serve as a forum to discuss policy issues in dispute.

(c) Meetings. The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) Administration.
(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.
(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).
(3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.
(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Sec. 5.6. General Responsibilities. Heads of agencies that originate or handle classified information shall: (a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order; (b) commit necessary resources to the effective implementation of the program established under this order; and (c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:
(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;
(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;
(3) establishing and maintaining security education and training programs;
(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;
(5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;
(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;
(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information;
(8) accounting for the costs associated with the implementation of this order,
which shall be reported to the Director of the Information Security Oversight Office for publication; and
(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.7. Sanctions. (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:
(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;
(2) classify or continue the classification of information in violation of this order or any implementing directive;
(3) create or continue a special access program contrary to the requirements of this order; or
(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:
(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and
(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

Sec. 6.1. General Provisions. (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. “Restricted Data” and “Formerly Restricted Data” shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Sec. 6.2. Effective Date. This order shall become effective 180 days from the date of this order.

William J. Clinton
The White House, April 17, 1995.

[Filed with the Office of the Federal Register, 2:04 p.m., April 18, 1995]

NOTE: This Executive order was published in the Federal Register on April 20.
**Statement on the Crash of an Air Force C-21 in Alabama**
April 18, 1995

Hillary and I were very saddened to learn of the crash of an Air Force C-21 aircraft near Alexander City, Alabama, last night, with the loss of eight lives. The death of these individuals is a tragic loss for the U.S. Air Force and the Nation. Their death reminds us all how much we are indebted to those military and civilian personnel who serve in the defense of our Nation. Our hearts and our prayers go out to the families and friends of those who were killed.

**The President's News Conference**
April 18, 1995

The President. Good evening. Ladies and gentlemen, before we begin the press conference, I want to express on behalf of Hillary and myself our profoundest condolences to the families and to the loved ones of the eight Americans who were killed in the crash of the Air Force plane in Alabama last night.

Tonight I want to talk about welfare reform. But before I do, I'd like to take just a minute to put welfare reform into the context of what is going on now in the United States Congress. Before the Easter break, the House of Representatives produced a flurry of ideas and proposals. Some of them were good. Some need work. Some should be rejected. My job is to work with people of good faith in both parties, in both Houses, to do what is best for America.

I was not elected to produce a pile of vetoes. And the Congress was not elected to produce a pile of political issues for the next election. My philosophy is that we have to go beyond this kind of politics-as-usual, the old debate about whether there should be more Government or less Government. I think we need a better and different Government that helps people who are helping themselves, one that offers opportunity but demands responsibility.

I have some common goals with the new Republican majority in the Congress. They say they want to reduce the deficit and the size of Government. I support that. My administration has reduced the deficit by $600 billion and is reducing the size of Government by over 250,000 people. In fact, if it were not for the interest we have to pay on the debt run up between 1981 and 1992, our Government's budget would be in balance today. Let me say that again, because I don't think the American people know that. If it were not for the interest we have to pay this year on the debt run up between 1981 and 1992, our Government's budget would be in balance today.

The Republicans say that they want to be tough on crime. Our crime bill is tough on crime, and I want to work with them to build on that. The Republicans are supporting the line-item veto, and so am I. I worked hard to get a version of the line-item veto passed through the Senate, and I look forward to working with them, actually getting agreement in both Houses and having a line-item veto come into law.

As we look ahead, the issue is, what are we going to do on the outstanding matters? I have commented at length on them before the newspaper editors, but let me say again, I want us to show responsibility and common sense and decency. Do we need to cut regulation, as they say? Of course, we do. But we don't need to undermine our commitment to the safety of our skies or the purity of our water and air or the sanctity of our long-term commitment to the environment. Do we need to be tough on crime? Of course, we do, but we don't need to repeal the commitment to 100,000 police officers or the assault weapons ban. Do we need to cut taxes? I believe we do, but not as much as the House bill provides. I think the tax cuts should be targeted to the middle class and to education so we raise incomes and growth for America over the long run.

Now let's talk a little about welfare. That's an issue that the Republicans and I, and the congressional Democrats should be able to agree on. They say we should end welfare as we know it. That's a commitment I made in 1992 and again in 1993 and 1994. Welfare reform is surely an example where all the people ought to be able to get together in the Congress to have reform.

We all know what we need. We need time limits for welfare recipients. We need strict