Controlled Unclassified Information;
Government Bureaucracy Out of Control

A White Paper July 2017
By: Harry Cooper

President Obama signed Executive Order 13556 with the promise to:

> "[establish] an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended". This preamble went on to say: "At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues".[1] This Executive Order creating Controlled Unclassified Information was intended by President Obama to fix these perceived problems with information sharing.

The public optic espoused in the Executive Order and restated many times by the Executive Branch agency responsible for implementation; that this new program will improve openness, create better government efficiency, and remove impediments to information sharing is diametrically opposed to the real impact of this new program.

The truth is that this new program creates yet another layer of secrecy, will cost taxpayers hundreds of millions of dollars, will not improve information sharing, and enumerates over 400 reasons for keeping government information from the American people. This was certainly not what President Obama intended, but the Executive Order itself is bereft of details and a government bureaucracy left to its own devices only makes things more complicated and less efficient.

Under the Freedom of Information Act (FOIA) the government may exempt from release (citing provision (b)(3)) any information protected by law from public access. Agencies, prior to implementation of CUI, relied on only a few laws to protect information from public access. Because the CUI program requires that government employees identify which one of over 400 laws regulations and government policies apply to the information. The regulation also requires that they mark the information in a way that ensures readers know that a law applies to protection of the information.

The public optic provided by both NARA and DOJ suggests that CUI is not a means to protect information under FOIA. The reality, however, is that once a government employee identifies a law that protects information from public access the FOIA reviewer has little choice but to use exemption (b)(3) to block public access to the information. Without CUI there is no marking to identify specific laws blocking access and government reviewers often missed those obscure laws that could potentially block access. The full implementation of CUI will likely cause an expansion

[1] EO 13556, President Barak Obama, Signed November 4th, 2010

of the use of (b)(3) and as a result information that would have been released prior to CUI will now be protected from release.

The cost to implement CUI is also staggering and will be yet a new burden on the American taxpayer. Agencies now must provide training to over 5 million government employees and government contractors. Each employee and contractor handling government information will be required to identify the law or laws that might protect information and apply appropriate markings to every document created. It is anticipated that several hours of training will be required for each employee. The cost for the resulting 10 million hours employees spend in training will easily top $750 million[2] when all hourly costs for employees are considered. The impact also includes 10 million less hours spent by employees and contractors doing the business of government and fighting terrorism.

All electronic systems used by federal agencies and federal contractors will have to be configured to apply the new CUI markings. Additionally, the CUI program requires all federal systems handling CUI to meet a moderate confidentiality standard established by the National Institute of Standards (NIST Standard 800-53) and contractor systems must meet a similar standard. While many agencies and contractors already meet these standards, those that do not must significantly increase the security of their Internet-based systems that have been used to handle unclassified information. When the various laws or regulations specify how access to information must be handled, electronic systems will need to be configured to apply these standards based on the markings that government employees or contractors have applied. This is a substantial increase in security over the current requirements and costs for government agencies and government contractors will all be passed along to the taxpayers.

The elimination of the current markings used on unclassified information (e.g. FOUO or LES) also includes a requirement to remark all legacy information unless an agency official waives the requirement to remark the information. Any decision by an agency to review information created before the implementation of CUI and apply the new markings will be very expensive and will also take personnel away from the agency's primary mission.

So, What Happened?

The need for common standards to protect unclassified information became apparent during the Bush administration shortly after 9/11. Expanded sharing of threat information with State, Local, Tribal and private sector entities also exposed these entities to the labyrinthine government bureaucracy where each agency had different rules for the protection of sensitive – but unclassified – information. In a memorandum sent to federal agencies President Bush asked that agencies find common standards for the protection of terrorism threat information sent to non-federal partners so a single, and simple, way to protect this information could be found and become the national standard.

[2] The GPO estimated the cost of average federal salaries at $123,000 in 2015. Contractors supporting the federal government generally cost about $300,000 per man-year with benefits and company profit figured in. The figure used in this paper ($75.00 per hour average) is based on a composite federal and contractor salary of $156,000 per year.

After several years of bureaucratic hand-wringing no single standard could be identified. Many agencies were unwilling to either reduce or increase the protection standards they created and the federal bureaucracy reached an impasse with respect to a single standard for protecting sensitive information that did not rise to the level of national security classification.

The Obama Administration picked up where the Bush Administration ended and more hand-wringing ensued. A very long and complicated Executive Order was drafted and the Oval Office quickly rejected it as it seemed to be the creation of another classification system. The long and complicated EO was replaced in a matter of weeks with a 2½ page Order that broadened the scope to all government unclassified information (not just terrorism threat reporting) and left all implementation details to the Information Security Oversight Office, a division of the National Archives.

Over the course of 5 years of government meetings and somewhat one-sided negotiation the National Archives finally published in 2016 a 45-page regulation that implements the 2½ page Executive Order. NARA also identified a list of 433 laws, regulations and policies that in some way compel federal agencies to protect information that is otherwise unclassified[3]. Each of these rules was given an abbreviation or indicator and each was also listed as either requiring "Basic" protection or "Specified" protection. Some laws are similar and were grouped, but the result was an initial list of 129 possible markings with 47 of them having additional "specified" handling requirements. Protection of this information may include some very specific dissemination requirements (e.g. sharing with foreign governments prohibited) or may even require that organizations or individuals authorized to see the information be on a list attached to the primary document.

The CUI federal regulation[4] that was published in 2016 requires initial and periodic training, establishes a challenge procedure for employees who question why information is marked as CUI, requires agencies to comply with the CUI Registry marking standards, and establishes regular annual reporting to NARA and to the President. The regulation also compels following NIST standards for electronic systems and provides safeguarding standards for paper-based storage of CUI information.

Is All This Necessary?

Probably not. In fairness to both President Bush and President Obama, a single and simple way to protect information that is not classified, but should not be published was needed. Common markings such as FOUO (For Official Use Only) and LES (Law Enforcement Sensitive) could have been kept and a single means to protect such information could have been created. Agencies should apply these markings when a law or regulation requires or permits agencies to protect the information from public access. Safeguarding can be managed at two or three levels that range from taking rudimentary steps to prevent public access, to simple safeguarding such as a locked room or desk drawer, or even – for the most sensitive information -- a list of authorized recipients. As long as the requirements are printed on the document in plain English very little training would

[3] The CUI Registry is found at: https://www.archives.gov/cui/registry/category-list
[4] 32 CFR 2002; 14 September 2016: https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information

be required. Agencies should be asked to improve electronic systems to limit the potential for unauthorized access, but the standards should be risk-based and agency driven rather than specified in a register.

While the protection of unclassified terrorist threat information that was sent to non-government partners needed a single standard for safeguarding, the overall program for handling unclassified government information was not broken. There have been no sensational losses of such threat information, no egregious failures to protect sensitive unclassified information and no problems caused by not having 129 different markings for unclassified information. Steps have already been taken to protect privacy information related to American citizens.

The Real Optic

Controlled Unclassified Information is a fundamentally good idea that has gone awry in an attempt by government bureaucrats to make it better. Identifying over 400 reasons to mark information as protected can have only one impact on transparency; the public will be denied access to far more information now than ever before. If a law says that information must or can be protected and a government bureaucrat dutifully marks the information with its corresponding code, it is very hard to imagine that the bureaucrat charged with deciding if information can be released under FOIA will do anything except apply the exemption.

The myriad markings, that look very much like classification markings, will certainly confuse almost everyone in government and information so marked will likely be disseminated far less and reach fewer people than information today that is marked as FOUO. Unclassified information today does not have the range of limits that are proposed for the new CUI. New CUI documents will be marked for release to specific foreign countries (not given to all foreign partners), dissemination limitations now also include Federal Government Only, No Contractors, or listed persons only. These are greater – certainly not lesser – controls on information than we have today.

The taxpayers would be well served if the new Director of the Information Security Oversight Office in NARA takes a step back and assesses the real impact of CUI on federal agencies, transparency, and the taxpayers. With a renewed effort, this program can still meet the objectives that President Obama envisioned in a much more efficient way than the current regulations provide for.

The author is a retired CIA official who has over 30 years of experience in managing national security classification programs. He participated in the drafting of the Presidential Executive Orders and federal regulations related to classification and secrecy. He is also the author of numerous white papers on national security classification. This manuscript was approved by CIA for publication in accordance with the author's secrecy agreement and CIA regulations.