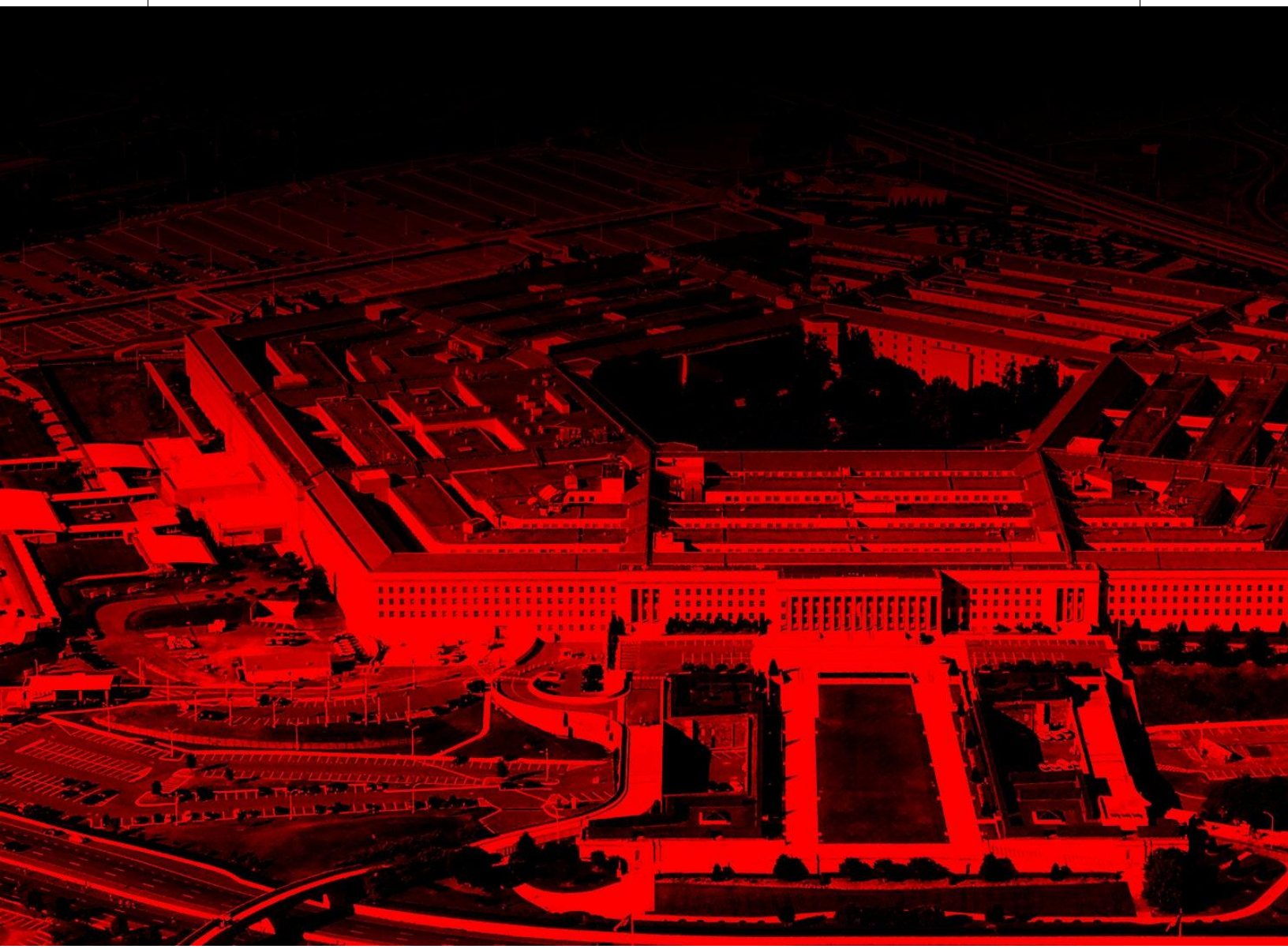
Special Access Programs and the Pentagon's Ecosystem of Secrecy

We shed light on the dark realm of the Department of Defense's often misunderstood classified apparatus in this comprehensive explainer.

TIM MCMILLAN AND TYLER ROGOWAY



To a lot of people, terms like “black budget,” or “black projects,” inspire dark imagery of government figures operating in contrast to the principles of a free and open society. Indeed, with tens of billions set aside every year for classified Pentagon programs and operations, it would be reckless of the public not to be willing to question that which they pay for, but lack the privilege of knowing anything about.

Inherently enigmatic and often grossly misunderstood, *The War Zone* set out to shed light on the obscure processes that are involved in maintaining the highly intricate ecosystem that works to guard the Pentagon’s most closely held secrets.

Special Access Programs: A Hidden World Most Will Never See

For the better part of the last twenty-five years, the manner in which the U.S. government safeguards and restricts access to highly classified information has been through a set of compartmentalization protocols termed “Special Access Programs.” Thanks to the government’s love affair with condensing words, most people are likely familiar with this formalized system of security’s acronym—”SAP.”

For most of us stuck on the outside trying to get an idea of what’s inside, the term “Special Access Program” is often misunderstood as being itself a classification level. In truth, SAPs are merely a set of security protocols limiting access of sensitive information to only authorized and necessary individuals. Cue the cliché, “That information is need to know, and you don’t have a need to know!”

Now, before one can gain a real appreciation for how Special Access Programs operate, like any scholar of history will tell you, “To understand the present, one must first appreciate the past.”

~~TOP SECRET~~

CONTROL NO. BYE 4544-67 #5

REFERRED TO OFFICE	RECEIVED			RELEASED		SEEN BY	
	SIGNATURE	DATE	TIME	DATE	TIME	NAME & OFFICE SYMBOL	DATE
ER via RB							

(OVER)

Handle Via Indicated Controls

BYEMAN- TALENT -KEYHOLE-COMINT

.....

.....

.....

Access to this document will be restricted to those persons cleared for the specific projects;

....

....

WARNING

This document contains information affecting the national security of the United States within the meaning of the espionage laws U. S. Code Title 18, Sections 793, 794 and 798. The law prohibits its transmission or the revelation of its contents in any manner to an unauthorized person, as well as its use in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States. It is to be seen only by personnel especially indoctrinated and authorized to receive information in the designated control channels. Its security must be maintained in accordance with regulations pertaining to the BYEMAN-TALENT-KEYHOLE and Communications Intelligence Controls. No action is to be taken on any communications intelligence which may be contained herein, regardless of the advantage to be gained, if such action might have the effect of revealing the existence and nature of the source, unless such action is first approved by the appropriate authority.

~~TOP SECRET~~

GROUP 1
Excluded from automatic downgrading and declassification

Top Secret cover sheet circa 1967., *CIA*

How National Security Information Is Classified

The early origins of Special Access Programs can be traced to March 22, 1940, when President Franklin D. Roosevelt signed Executive Order 8381, creating for the first time, three security designations for America's most crucial information—restricted, confidential, and secret.

In the ensuing years, various presidential executive orders have tweaked how the government designates classified information. The current levels of classification are confidential, secret, and top secret. The determining factor for how information is classified depends on how much damage an unauthorized disclosure would reasonably be expected to cause.

- **Top Secret:** "Exceptionally grave damage to national security."
- **Secret:** "Serious damage to national security."
- **Confidential:** "Damage to national security."

Important to note, established through the Atomic Energy Act of 1954, the Department of Energy (DOE) uses two differing equivalent levels of security clearance.

- **Q-Clearance:** Equivalent to a Top-Secret level clearance.
- **L-Clearance:** Equivalent to a Secret level clearance.

For clarity's sake, at times misrepresented by the entertainment industry, a "Yankee White clearance" is not an actual security clearance. "Yankee White" is an administrative nickname for the background check performed for persons who will work within close proximity to the President or Vice President. According to Department of Defense instructions, to obtain a Yankee White clearance one must pass the same Single Scope Background Investigation (SSBI) necessary for a top secret clearance, and establish "unquestionable loyalty to the United States."

Within the world of SAPs, a program can involve information from any one of these official classification levels. Further adding to the confusion, in many cases, a single Special Access Program will contain multiple components, each with differing classification levels.

The Dubious Origins Of Special Access Programs

The incredulous mystique surrounding SAPs likely comes from the unofficial, ad hoc nature of their origins. In 1953, when President Dwight D. Eisenhower issued Executive order 10501, he eliminated classification authority from 28 government entities, limiting only departments and agencies of the executive branch the ability to classify materials. More importantly, President Eisenhower's directive removed the previously approved "restricted" designation.

President Dwight D. Eisenhower in the Oval Office. , *Eisenhower Library*

Up to this point, “restricted” classifications functioned as a means of limiting certain information from people who may indeed have held an active security clearance; however, they didn’t have a “need to know.”

In light of being given a formal order by the Commander-in-Chief, some departments within the Pentagon weren’t all that keen on being unable to limit access to their secrets. In response, many

agencies began to unofficially use "special access." Albeit with no official authority, these informal "special access" classifications would allow for the continuance of closely guarded, tight-knit programs to be hidden within the government.

Now, it's hard to argue that the flagrant rejection of national directives wasn't a recipe for disaster waiting to happen. In fact, it's likely no coincidence that some of the darkest times in government secrecy went on during these unofficial "special access" years. For example, the CIA's infamous Project MKULtra began in 1953 and remained active until 1973. Coincidentally, 1973 was the same year that, during an oversight hearing, a report by the Committee on Government Operations brought to light that dozens of unauthorized "special access, distribution, control labels, stamps, or markings" were being used by "many executive agencies having classification authority and dozens of other agencies that do not possess such authority."

In all fairness, by the time of their discovery, the precedent of unofficial special access programs was primarily a moot point. Either intentionally or by ironic happenstance, three months before five men being caught breaking into the Democratic party headquarters at the Watergate complex in Washington D.C., on March 8, 1972, President Richard Nixon signed Executive Order 11652, legitimizing and establishing the overall framework for what would eventually become the "Special Access Program" of today.

Still not thoroughly having worked the kinks out, according to the Center for Development of Security Excellence's (CDSE) Special Access Programs Training Course, from the early 1970s to 1980s, SAPs—referenced even within the government as "black programs,"—were almost exclusively restricted to safeguarding DoD acquisition programs. In fact, the existence of "black programs" wasn't publicly known until the mid-1980s, when the controversial "Project Yellow Fruit" unceremoniously thrust government secrecy programs in the limelight.

More on "Project Yellow Fruit" to come.

By the mid-1990s, these enigmatic workshops shed the "black program" moniker, opting to go by the more contemporarily familiar "Special Access Program." In addition to the more dexterously sleek title, intelligence, operations, and support programs were added to the SAP repertoire, establishing the Special Access Program regime we've come to know today.

Armed with some history on SAP's, let's take a look at how they operate.

Enter the Bureaucratic Jungle of SAPs

When considering the term "special access program," typically, people envision one of the three categories that go on within the Department of Defense, as outlined by DoD 5205.07. Acquisition, intelligence, operations, and support. Breaking these categories down to gain a sense of what they entail:

- **Acquisition SAPs:** Programs that involve research, development, testing, modification, evaluation or procurement of new technologies. (According to the CDSE, Acquisition SAPs make up 75-80% of all DoD SAPs)

- **Intelligence SAPs:** Planning and execution of, especially sensitive, intelligence or counter-intelligence operations.

- **Operations and Support SAPs:** Planning, implementation, and support of sensitive military activities.

It's important to note that, though the DoD's three main categories are the most well-known, Special Access Programs are inherently just a procedure within the government. In fact, there are many other categories of SAPs that go on outside the DoD. For example, the Secret Service's Presidential travel support detail is technically a SAP. Additionally, within the intelligence services, these similar sets of protocols are termed "Sensitive Compartmented Information" (SCI) and not "Special Access Programs."

Additionally, separate from an objective category, all special access programs fall under one of two distinctive protection levels—" acknowledged" and "unacknowledged."

- **Acknowledged SAPs** – Programs whose existence and purpose can be openly recognized. With acknowledged SAPs, typically only intimate details, such as technologies, materials, or techniques, are kept secret. Funding for acknowledged SAPs is mostly unclassified and can be readily seen in the government's fiscal budget.

With its existence well known, yet its inner details still remaining mysterious, Northrop Grumman's B-21 Raider is an excellent example of an Acknowledged Special Access Program actively going on today.

On the other end of the spectrum, serving as the inspiration for much spy fiction or conspiracy theories of secret space forces, there is the "Unacknowledged" SAP.

- **Unacknowledged SAPs or "USAPs":** The shy sibling of the SAP family. When a SAP is designated as "unacknowledged" not only is a program's purpose carefully guarded, as the name implies, USAPs mere existence may be denied to everyone but a spare few who aren't a part of the program. Given their shadowy presence, it should come as no surprise, the funding for unacknowledged SAPs is either classified or is intentionally hidden within the Federal budget.

An example of an Unacknowledged SAP would be the RQ-170 before it was officially disclosed to the public.

In rare instances, when information is considered to be of the most extremely sensitive in nature, the Secretary of Defense can formally exempt a program from federal reporting requirements and establish the pinnacle of secrecy—the "Waived Unacknowledged SAP."

Due to their ultra-secretive nature, Unacknowledged or Waived-Unacknowledged SAPs, serve as fertile breeding grounds for conspiracies of hidden crashed UFO technology or veiled government "carve-outs" whereby the general public's benefit is an afterthought. In truth, USAPs or Waived USAPs, like anything else that lacks accessible, verifiable facts, are likely

very mythicized. With that said, like any good myth, there's some truth and historical precedent that give legitimate reasons to be concerned with these deeply hidden programs.

With that in mind, let's take a quick journey back to the not-too-distant past. To a time that shows Special Access Programs have, and can, operate in a manner opposed to public interest.

"Yellow Fruit," The Rogue SAP The Government Wants To Forget

In 1983, an arbitrary internal audit turned up enormous inconsistencies in an unacknowledged, covert SAP being run out of the newly formed Special Operations Division of the DoD. Code-named "Yellow Fruit," the program was established to provide additional operational security and counter-intelligence assistance for missions in Central America. Yellow Fruit was a genuine "deep cover" USAP, with the program's director, former Assistant Chief of Staff for Intelligence, Lt. Col. Dale Duncan, outwardly appearing to have "retired" from the Army to start a private consulting firm called Business Security International.

The discovery of financial discrepancies in Yellow Fruit sparked a formal investigation by the FBI. The inquiry into Yellow Fruit would result in Lt. Col. Duncan, Special Operations Division Commander Lt. Col. James E. Longhofer, and several other members of SOD being court-martialed for a hodgepodge of varying crimes. In addition, many never-fully proven allegations, such as millions of stolen dollars hidden in Swiss bank accounts, set-ups of other U.S. military officials with prostitutes and hidden cameras, and even ties to the Iran-Contra affair, still loom over Yellow Fruit.

Though career military officers allowing their moral compasses to diverge from pointing ethically north is somberly disappointing, it's regrettably far from unprecedented. Instead, what made Yellow Fruit such a significant turning point in the formative growth of current classified operations came from the embarrassing lack of DoD control and oversight that was revealed.

As the rotting stench of Yellow Fruit made its way up the military hierarchy, top Army leadership, including Army Chief of Staff John Wickham and his Vice Maxwell Thurman, were stunned. The level of shock conveyed from the Pentagon's leadership was understandable when you consider that in "The Dilemma of Covert Action," published by the U.S. Army War College in 1989, it's said none of the DoD brass had ever been briefed on the program and literally had no clue that a mere 15-minute drive from the Pentagon, tucked amongst a suite of commercial offices, a multi-million-dollar clandestine military operation was being run.

Determining exactly what all went on within Project Yellow Fruit can prove to be a rather difficult task. Spare a few newspaper articles from the 1980s, and publicly available information is extremely limited. With that said, the required CDSE's training course for all persons participating in DoD SAPs, repeatedly mentions "Yellow Fruit" as being an inspiration for a wave of oversight and controls put in place to stem the ability for a small group within government to literally go rogue.

The Inner Workings of Special Access Programs

In the Department of Defense's mind-numbing behemoth of formal policies and directives, five volumes totaling 151 pages are now dedicated solely to Special Access Programs. Of course, if a light book's worth of reading wasn't enough, there are also specialized manuals for many divisions within the Pentagon that also provide their own expansive volume of rules and regulations.

For example, there's a Joint Army-Navy-Air Force SAP manual, offering service members of these three branches an extra 129 pages of supplemental reading. Lest we forget, since a significant amount of secret government activity is farmed out to private industry, government contractors who are involved with SAPs get their own 131 pages of "National Industrial Security Program" operating manual to peruse.

Needless to say, though a considerable amount of the government's covert goings-on are indeed hidden from prying eyes, substantially more regulation and control have been implemented since the days when Project Yellow Fruit was turning in $56,000 receipts for desk calculators.

A word of note before proceeding, for all those fans of flowcharts, this would be an excellent time to break out the markers and whiteboard, because as promised, no matter how "unconventional" SAPs may be, at the end of the day, they're still subject to all of the customary administrative confusion that's characteristic of civil service.

Courtesy photo by Petty Officer 1st Class Brandan Schulze

Special Access Program Central Offices

Within the DoD, the Secretary or Under Secretary of Defense is the principal authority for all Special Access Programs. Assisting the military's Chief Executives in this endeavor involves a vast complex of ministerial powers.

Serving on the front lines of the secrecy mosaic is the "Special Access Program Central Offices" (SAPCO). With a process that thrives on compartmentalization, it should come as no surprise, by "central," the DoD actually means there are three different types of SAP Central Offices residing

in the corridors of the Pentagon—Component-Level SAPCOs, OSD-Level SAPCO, and DoD-Level SAPCO.

- **Component-Level SAP Central Office (SAPCO):** They can be found within each branch of the military, the Joint Chiefs of Staff, the Defense Advanced Research Projects Agency (DARPA), and the Missile Defense Agency (MDA). The Component-Level SAPCOs are responsible for initiating the prospective process for assessing the need for a Special Access Program. Once a SAP has been established, a Component-Level SAP Central Office serves as the hands-on manager for the SAPs that fall under its purview.

- **Office of the Secretary of Defense-Level SAP Central Office (OSD SAPCO):** Specifically established to assist the Deputy Secretary of Defense, the Office of the Secretary of Defense-Level Central Office serves as the oversight authority for all SAPs.

- **Department of Defense SAP Central Office (DOD SAPCO):** Serving to help streamline this entire fragmented and confusing process, the Department of Defense SAP Central Office functions as an ambassador by communicating and advising agencies of the executive branch and Congress on all issues relating to SAPs.

Now, if that wasn't enough delegated authority for you, have no fear, because roaring alongside the SAP Central Offices like forking whitewater rapids of procedural hierarchy comes the "SAP governance structure."

The Special Access Program Governance Structure

Spearheading the SAP governance structure is the SAP Oversight Committee (SAPOC). Made up of a who's who of Pentagon Under Secretaries, Vice Chiefs, and Assistant Directors, the Oversight Committee's primary role is to advise and assist the Secretary and Deputy Secretary of Defense in the governance, management, and oversight of all DoD Special Access Programs.

Ensuring that the limitation of secrecy to only a select few isn't a decision made in a vacuum, assisting the SAP Oversight Committee is:

- **Senior Review Group (SRG):** The principal working-level body who governs the process of SAP oversight.

- **SAP Senior Working Group (SWG):** Provides recommendations to the Senior Review Group and serves as a senior program protection forum coordinating, deconflicting, and integrating special programs.

Pausing for a moment to take a breath, don't put down those markers and flowchart just yet. As twisting and turning as all the aforementioned regulatory authorities might be, we're far from having the whole picture of the Special Access Program process.

The Importance Of Maintaining Secrecy

In the late 1970's NASA began operating an extensively modified Boeing 747 airliner to ferry the Space Shuttle around. By the late 1980s, two were in operation. Unimaginatively, these modified jumbo jets were called the "Shuttle Carrier Aircraft" (SCA).

SCA with an Orbiter on its back., *NASA*

A decade after NASA began toting around the Space Shuttle Orbiter on the back of a wide-body plane, Russia started soaring through the skies in their brand new Antonov An-225 Mriya (meaning "dream" in English).

Powered by six turbofan engines, the Mriya, to date, is the heaviest aircraft ever built. Oh, and as it happens, the Mriya was built to offer piggyback rides to Russia's own space shuttle, the Buran. In case you don't see where this is going, according to the Center for Development Security Excellence (CDSE), it was later determined that Russia had "borrowed" technical information on the SCA to help develop their own massive orbiter transport aircraft.

Protecting technological advancement isn't just about maintaining military dominance. Instead, in terms of time and developmental dollars, the cost associated with the loss of industrial secrets can be enormous. When Russia "acquired" the fine technological details to develop the An-225

to carry their version of the Space Shuttle Orbiter, the Soviet Union effectively saved itself considerable time and money at America's expense. Noting only one Mriya has ever been built, the argument can be made, without the unwilling help of the U.S. aerospace industry, that Russia's shuttle ferry may never have entered operation.

Photo taken at the 38th Paris International Air and Space Show at Le Bourget Airfield showing a line-up to tour a Soviet An-225 Mirya aircraft that is carrying the Space Shuttle Buran on its back. June 12, 1989. , *Master Sgt. Dave Casey/Public Domain.*

Ultimately, examples like Russia's An-225 serve as distinct reminders that the most vital part of protecting national secrets doesn't necessarily occur at desks and in boardrooms of the Pentagon. Instead, it goes on within the Special Access Programs themselves.

Securing Special Access Programs

In all fairness, with the intelligence field supposedly being one of the last bastions of "gentleman warfare," it's safe to assume America has its fair share of hush-hush programs geared at "borrowing" other nations' research and development. In fact, known past and present Foreign Materiel Exploitation (FME) programs alone are shining examples of this.

That aside, in the span of SAP controls, the Office for the Under Secretary of Defense for Intelligence (OUSDi) SAP Control Office fills the very vital role of monitoring and investigating counter-intelligence matters, security violations, or infractions within all DoD SAPS.

Assisting OSDi's Central SAP Office in this effort is the Office of the Director of National Intelligence and the powerful 17 individual agencies that make up the United States intelligence community. Bolstering this mighty SAP Central Office, the U.S. Defense Security Service (DSS) helps provide operational support and security oversight for all DoD SAPs.

Of course, the first line of defense in protecting the integrity of SAP secrecy starts with who is granted access to a program. Regardless, if a person is in the military, a federal-civilian employee, or a private contractor, several prerequisites must be met before one can work within a SAP.

Working Inside A SAP

The path to working in a SAP begins with a currently accessed person nominating a potential candidate to the "access approval authority," or the central office that the SAP emerges out of. If a candidate does not presently possess an active secret or top-secret clearance, the appropriate clearance must be obtained before one can be considered for involvement.

Finally, all persons who will be involved in a SAP must agree to be subject to random "counter-intelligence scope" polygraph examinations and sign a DoD-approved SAP indoctrination and non-disclosure agreement.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN _____ AND THE UNITED STATES

(Name of individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, *952 and 1924, title 18, United States Code; *the provisions of section 783(b), title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

STANDARD FORM 312 (Rev. 7-2013)
Prescribed by ODNI
32 CFR PART 2001.80 E.O. 13526

DoD Document

Once inside a special access program, there are yet still several vital roles that help ensure the secure integrity of each individual program. Some of these are:

- **The Government Program Manager (GPM), and their private industry equivalent, the Contractor Program Manager (CPM):** The person who manages all overall aspects of a specific program.

- **Program Security Officer:** The person responsible for all aspects of security in the program. Every SAP has a PSO, however, large or complex SAPS can also have

additional Government SAP security officers or contractor program security officers to assist the Program Security Officer.

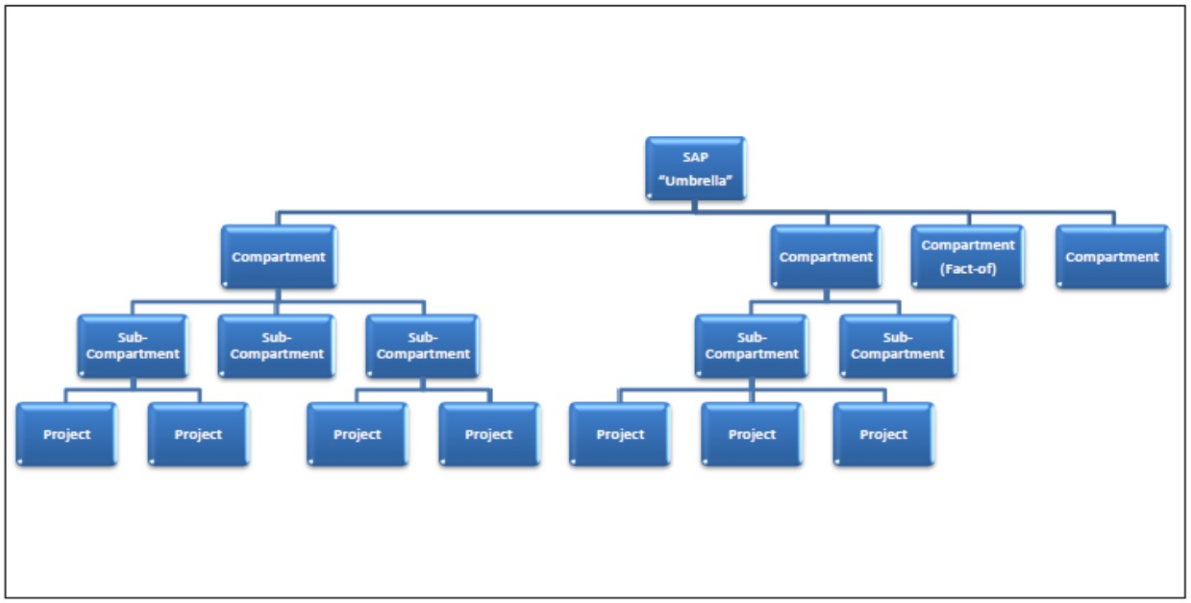
Further protecting who knows what, a SAP's overarching scope and purpose can fall under one program "umbrella." However, multiple compartments, which can further break down into separate sub-compartments, and finally, numerous projects, can all emerge from under a single SAP umbrella.

It's entirely possible for a compartment, sub-compartment, or project not to have access, or even to be aware of the work that's going on in other sections of the same SAP.

When it comes to the extreme isolation of work, it's not just about keeping information out of the hands of foreign adversaries. Sometimes components are cordoned off from each other because you may have two different contract partners from the same industry working on different aspects of a SAP. In essence, caution must also be taken to ensure industrial partners don't "borrow" each other's trade secrets.

DoDI 5205.11, February 6, 2013

Figure 1. Sample Hierarchy



Sample SAP hierarchy; Source: Department of Defense, DoDI 5205.11

DoD graphic

Oversight Of Special Access Programs

All Special Access Programs are subject to federal and defense acquisition regulations. As such, all SAPs can be audited and inspected by a host of oversight entities, including the Government Accountability Office or the DoD Inspector General.

Equally, oversight of SAPs isn't merely left to agency policies and directives. Instead, it's a matter of federal law, as defined by Section 119, Title 10 United States Code.

By federal statute, all active acknowledged and non-waived unacknowledged Special Access Programs must submit reports to the House and Senate Authorization, Appropriations, and Intelligence Committees annually. These yearly reports provide committee members with an estimated total budget request for the upcoming fiscal year, a brief description of the program, including the number of persons involved, the status of significant milestones or current issues, and the actual cost of the program for each previous fiscal year.

Any member not assigned to one of the defense or intelligence committees may be granted access to non-waived SAPs, provided they receive permission by the ranking and minority member from each of the respective committees and with approval by the Secretary or Deputy Secretary of Defense.

But What About Those Waived-Unacknowledged SAPs?

As mentioned earlier, in rare instances, when a SAP's purpose and scope are deemed so sensitive that standard reporting procedures could pose a risk to national security, the Secretary of Defense can authorize the darkest of "black programs," the waived-unacknowledged special access program.

According to the Center for Development of Security Excellence, "Waived SAPs have more restrictive reporting requirements and access controls." Determining what precisely the CDSE means by this statement is a little tricky.

In the book, *Strategic Intelligence: Covert Action, Behind the Veils of Secret Foreign Policy*, author Lock K. Johnson notes, "Waived SAPs are only orally briefed to the so-called Gang of Eight, this is, the chair and ranking (minority) members of both the Senate and House intelligence (or Armed Services) committees, and House and Senate Majority and Minority Leaders." Sure to raise a few eyebrows, Johnson mentions that the National Security Agency's controversial "warrantless surveillance" program, which ran from 2001-2007, was a waived SAP.

According to the very limited information provided by the Department of Defense's Directive 5205.07, the "Access Approval Authority" for waived SAPs is narrowed down to the Deputy Secretary of Defense, Under Secretaries of Defense, or a component head with "cognizant authority."

Beyond this, even after combing through hundreds of pages of DoD directives, policies, and federal Title 10 and Title 50 laws, it's hard to pin down exactly how waived-USAPs are governed.

Indeed, since the self-indulgent days of Project Yellow Fruit, the DoD has piled a sizable number of regulations and policies governing the Special Access Program process. However, given the obscurity of even being able to determine how checks and balances are maintained with waived

USAPs, one cannot help but consider that risks may still lurk within the very murky waters of this bureaucratic swamp.

As we twist further down the spiral of sanctioned secrecy, let's take a look at some of the concerns with intensive secrecy that's governed by a mere few individuals.

The Dark Side Of An Already Dark World

Taking a glance at the DoD's mind-numbing number of rules, regulations, and directives pertaining to SAPs, it's not hard to see why the CDSE can make the claim that modern Special Access Programs have significantly more scrutiny and oversight than those of the past that may have been marked by somewhat laissez-faire attitudes. However, it would not be objectively fair not to point out that, even since the mid-1990s, there have been examples of mismanagement or corruption involving SAPs.

When it comes to the corruptibility of SAPs, leading the charge is the biblical "root of all evil," and the cold, hard fact that these programs of isolated secrecy can involve enormous amounts of money.

Just how enormous?

Well, according to the Stockholm International Peace Research Institute, the United States' $81.1 billion budget request for classified intelligence programs alone in 2019 is larger than nine of the next top-ten foreign nations' *total military expenditures*. Only China, with an estimated total defense budget of $250 billion U.S. dollars, exceeds the budgetary sum of America's intelligence community's classified budget. This does not include the tens of billions of dollars spent on the Pentagon's non-intelligence-related classified programs every year.

As staggering as having a classified budget that exceeds many countries' entire GDP might be, it *still* doesn't account for all the money being spent on secret programs.

A 2016 Office of Inspector General (OIG) report indicated the DoD couldn't account for *$21 trillion* in transactions and adjustments from 1998 to 2015. It's important to note that this movement of funds, an average of $1.2 trillion annually during this 17-year period, which was "unsupported" by accounting documentation, does not reflect any actual "missing" money that could have been funneled into "black programs" or SAPs. OIG also did not suggest that any of these funds had been categorically lost, stolen, or otherwise burned in ritual sacrifice.

At the same time, the U.S. military's apparent inability to properly record trillions of dollars' worth of transactions calls into question how well it is monitoring even its most basic financial activities to prevent money from ending up diverted or simply misspent. Historically, black programs have exploited the nebulous nature of U.S. government budgets to fund their efforts through complex arrangements involving multiple agencies, making a full accounting, or even any accounting, of their costs difficult.

So going back to that initial question, just how large is the sum of the money involved in these black programs?

We really don't know because it's seemingly *uncountable.* But it's safe to say that it is very large.

Considering how much of public politics is dominated by relentless bickering over the allocation of government funds, the potential for classified programs to have uncountable, perhaps even undefined, streams of cash is almost incomprehensible.

Corruption Breeds In Shadowy, Cash-Packed Environments

Access to large sums of difficult-to-track cash can have the unfortunate, yet all too common side-effect of tempting seemingly moral persons to engage in very immoral acts. Such was the case with former CIA executive Kyle "Dusty" Foggo, who was indicted in 2007 by the Department of Justice for accepting bribes in return for steering millions of taxpayer dollars towards his friend's private contract company, ADCS Inc. In the same case against Foggo, former California Congressman and Navy ace fighter pilot Randy "Duke" Cunningham was sentenced to 8 years in federal prison for his part in the procurement scam.

Absent any malicious intent, there are still areas within the SAP process that provide a safe haven for poor decision-making and insufficient oversight.

Chiefly, when it comes to America's elected leaders who are tasked with approving or disapproving of clandestine programs. How many of them actually possess the technical prowess to adequately assess a program's feasibility or need? Out of the members of "The Gang of Eight"—the only eight members of Congress who are authorized to have knowledge of Waived-Unacknowledged SAPs—presently, none have any background in the military or technological and scientific research sectors.

This reality is somewhat remarkable, considering one must possess the technical requisites necessary to work within a SAP, however, a significant number of the precious few who ultimately pull the strings of this hidden world outside of the Pentagon and the industrial complex that support it need only to be popular among their constituencies.

There are other potentially adverse aspects of secrecy that get very little attention. For instance, it costs exponentially more money to run a classified program than one that is unclassified. The deeper you get into the shadows, the more expensive that secrecy costs, and declassifying something can be extremely expensive, problematic, and time-consuming. This has likely resulted in throngs of programs that pose little to no risk when it comes to disclosure, but will never see the light of day regardless.

In addition, there have been accusations that some programs get classified at least in part so as not to compete with existing and, in some cases, inferior high-profile capabilities or

operations that are already in production or underway. It's possible that this could be to hide the program from those who would otherwise work to destroy it—especially the pork rollers on Capitol Hill and the highly territorial services that occupy the Pentagon. On the other hand, even a service itself could fear that its own clandestine emerging capability could threaten an existing one that it has already bet heavily on.

Bad Ideas, Big Classified Budgets

An argument can certainly be made that putting reclusive, highly complex, and expensive defense programs in the hands of elected leaders who lack any subject matter expertise makes for ideal conditions that result in costly and entirely avoidable failures. One example is the proposed nuclear-powered rocket system "Project Timber Wind."

Once considered a key component of President Reagan's Strategic Defense Initiative—better known as "Star Wars"—Timber Wind also offers a peek at how deep secrecy can lend a hand to quietly crossing the line of what the public is likely willing to find acceptable in the name of national security.

The aim of the once-unacknowledged SAP, Timber Wind, was to develop nuclear thermal rockets capable of reaching space to support ballistic missile defense. Outwardly unreasonable as it sounds, with America no longer facing the Cold War threat of the Soviet Union, in 1992 when details about the program were declassified, many in the scientific community were stunned to discover the grand plan behind Timber Wind involved a two-stage rocket process whereby, immense tanks of liquid hydrogen attached to a nuclear reactor would be fired off into the atmosphere.

Serving as the inspiration behind the founding of the Federation for American Scientists' (FAS) "Project on Government Secrecy," current FAS director Steven Aftergood would describe Timber Wind as "Just about as dangerous a machine as any I can imagine," adding the SAP was "Sheer scientific adventurism."

When all was said and done, the government shelled out $139 million before finally canceling Project Timber Wind. Though the loss of money may be significant, the potential costs for "pumping liquid hydrogen across a 'bed' of uranium at 5,000 degrees Fahrenheit," a mere stone's throw from an unwitting Nevada or Utah populous, could have resulted in far more catastrophic public health and ecological consequences.

Intriguingly, (in a macabre kind of way) a willingness to take extreme risk to maintain the vanguard defensive capabilities, isn't merely an isolated event. Instead, as many former Area-51 employees have come to discover, secrecy with minimal oversight can have very personal and disturbing consequences.

Area 51's notorious perimeter. , *X51/Wikicommons*

Area 51: A Place That Is Literally Above The Law

In the mid-1990s, several former employees of the Air Force's infamous Area 51 flight test facility—the developmental home of so many SAPs and a place that is itself a massive SAP—sought the help of legal scholar and attorney Jonathan Turley.

Riddled with various serious illnesses, the former Area 51 workers told Turley that officials had, for years, been burning classified equipment and materials in large trenches for disposal at the secret military facility located seventy-five miles north of Las Vegas, Nevada. The plumes of thick, toxic smoke that would billow and linger across the installation would come to be known as "London fog," by Area 51 employees, Turley later recounted.

Armed with tales of ecological catastrophe and a zeal for justice, Jonathan Turley and the Area 51 veterans would launch an epic legal battle to define the line between national security and basic civil liberties.

The chief aim of the Area 51 employees' lawsuit was to discover what exactly they had been exposed to, in hopes it might help them receive medical care. As reasonable as this request might have been, sanctioned secrecy protecting Area 51 not only allowed for the government to refuse information that might save the workers' lives, it also allowed for the government to repeatedly insist that no such place even existed.

Only after Turley provided satellite pictures he purchased from Russia did the government finally admit Area 51's existence to the courts. As a result, U.S. District Judge Phillip Pro would reject the government's claim of "state secrets privilege" and declare the government was required to disclose what hazardous chemicals employees had been exposed to.

In a tragic twist, in light of the federal court judge's ruling, no one would get the opportunity to ever find out exactly what types of toxic substances had been allowed to permeate the secret facility. Instead, in an 11th-hour intervention, President Bill Clinton issued a Presidential Determination that exempted installation from environmental disclosure laws.

Presidential Documents

Presidential Determination No. 95–45 of September 29, 1995

Presidential Determination on Classified Information Concerning the Air Force's Operating Location Near Groom Lake, Nevada

Memorandum for the Administrator of the Environmental Protection Agency [and] the Secretary of the Air Force

I find that it is in the paramount interest of the United States to exempt the United States Air Force's operating location near Groom Lake, Nevada (the subject of litigation in *Kasza v. Browner* (D. Nev. CV–S–94–795–PMP) and *Frost v. Perry* (D. Nev. CV–S–94–714–PMP)) from any applicable requirement for the disclosure to unauthorized persons of classified information concerning that operating location. Therefore, pursuant to 42 U.S.C. § 6961(a), I hereby exempt the Air Force's operating location near Groom Lake, Nevada from any Federal, State, interstate or local provision respecting control and abatement of solid waste or hazardous waste disposal that would require the disclosure of classified information concerning that operating location to any unauthorized person. This exemption shall be effective for the full one-year statutory period.

Nothing herein is intended to: (a) imply that in the absence of such a Presidential exemption, the Resource Conservation and Recovery Act (RCRA) or any other provision of law permits or requires disclosure of classified information to unauthorized persons; or (b) limit the applicability or enforcement of any requirement of law applicable to the Air Force's operating location near Groom Lake, Nevada, except those provisions, if any, that would require the disclosure of classified information.

The Secretary of the Air Force is authorized and directed to publish this Determination in the **Federal Register**.

William J. Clinton

THE WHITE HOUSE,
Washington, September 29, 1995.

[FR Doc. 95–25244
Filed 10–6–95; 10:54 am]
Billing code 3910–01–M

US Government Document

Ultimately, by a stroke of the pen, secrecy overrode the federal law, defeated basic civil liberties, and largely sealed the fates of those impacted by the open-air burnings at the base. Also, President Clinton put a definitive stop to any appeals for government accountability at the reclusive military test site.

Sadly, former Area 51 employees Wally Kasza and Bob Frost would lose their own personal battles with debilitating skin and respiratory illnesses. Analysis of tissue samples from the autopsy of Bob Frost showed "unidentifiable and exotic substances that one of the nation's premier scientists could not recognize," Jonathan Turley later told the L.A. Times. Described by Turley as "deeply patriotic guys," both men are assumed casualties of the government's war to maintain secrecy at Area 51.

Since the legal battles of the 1990s, more employees have continued to come forward complaining of serious and life-threatening ailments as a result of working at Area 51. Instead of making amends for the wanton risk placed on the very people who helped usher in some most remarkable advances in military technology the world's ever known, every U.S. president has annually reissued President Clinton's initial 1995 executive order declaring Area 51 to be above environmental laws.

While the potential for Special Access Programs to serve as hidden conduits for costly government waste can and should spark formal debate and even dinner table discussions, for the families of Wally Kasza, Bob Frost, and others who've found themselves dealing with the effects of extreme government secrecy, the price for that secrecy can come with significant and dramatic personal costs.

Dark Nights Can Equal Bright Stars

Now, as ominous as they may feel at the moment, Special Access Programs are far from being all doom and gloom. Conversely, as bestselling author Richard Paul Evans puts it, "It is often in the darkest skies that we see the brightest stars."

When it comes to bright stars set against a dark sky of secrecy, one must consider, arguably, the forefather example of the modern SAP—Lockheed's U-2 Dragon Lady high-altitude reconnaissance aircraft.

The minimal interference of working in the shadows allowed Kelly Johnson and his team of just 28 Lockheed special projects engineers to design, build, and fly a spy plane capable of flying at 70,000 feet in only 8 months. Ironically, the U-2 program also gave birth to Area 51.

U-2 testing at Groom Lake (what would become known as Area 51). , *CIA*

Employing many of the same techniques used by SAPs today, the extreme secrecy reduced external meddling from the powers that be in and around Washington D.C., the potential of competing interests from the military services, from the very entity the program is being executed for, and from multiple outside contractors. The latter of which allowed 87% of the U-2's development to be performed in a single building in Burbank, California, then the Skunk Works' headquarters.

Ultimately, deep secrecy can allow for wasteful "scientific adventurism," the bottom-line truth is that this same risky inspiration can equally allow for incredible technological breakthroughs. In fact, without the breathing room of secrecy and minimal external interference, some remarkable and game-changing technologies may never have come to fruition.

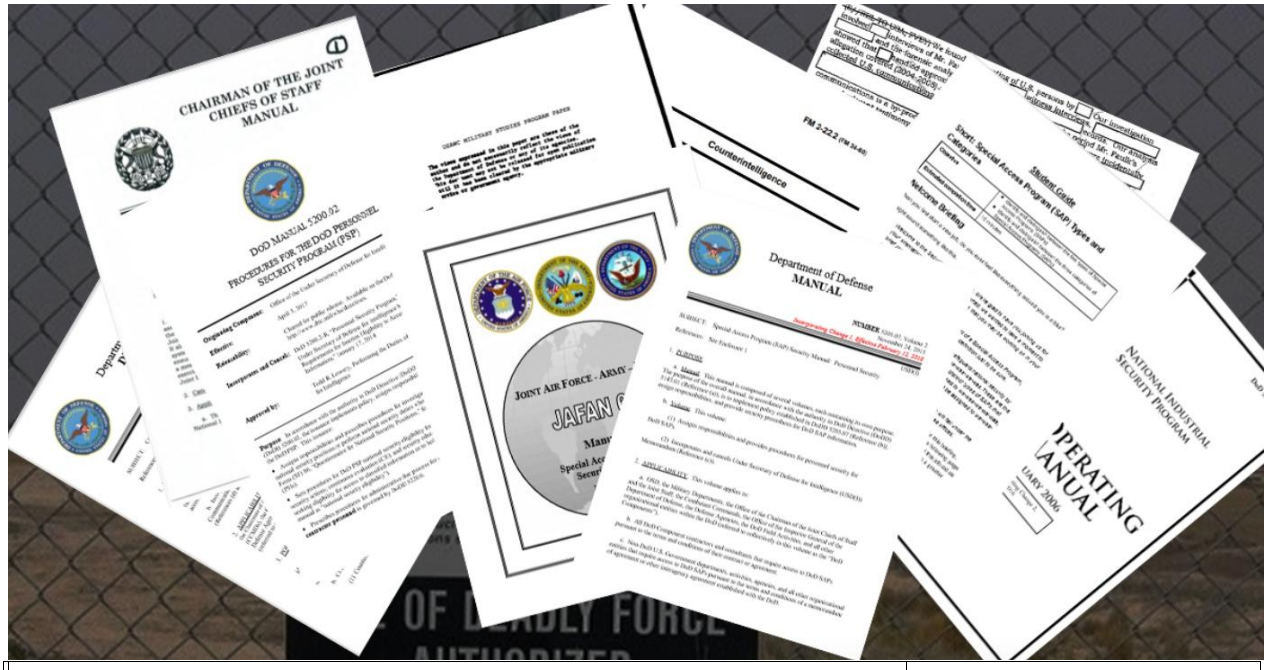
For instance, the F-117 Nighthawk and even the framework for the modern internet emerged from the dark shadows of Special Access Programs.

Whereas disclosed defense programs that fail after a bunch of money was spent can have major repercussions, even though some would say not major enough, secrecy allows for risks to be taken without the fear of becoming a headline news story.

Yes, this is a major concern for potential abuse and waste, but at the same time, it has become somewhat essential to making huge qualitative leaps in defense-related technologies. Lockheed's Skunk Works largely defined this reality and has built a hugely successful operational model around it that has been knocked off by many contractors and business entities.

To put it another way, making it ok to fail by classifying a program can be an incredibly powerful tool for promoting major innovation.

With all this in mind, it is simply impossible to ever say that innovation shrouded by secrecy is inherently a bad thing.



Final Thoughts on Special Access Programs

It's important to note, we've almost entirely focused on the Department of Defense's secrecy ecosystem and the Special Access Programs and "clandestine" operations that spring forth from it. Though briefly mentioned early on, when it comes to secrets stemming from the intelligence community and "covert" activities, that's a whole other sprawling government maze, complete with entirely different regulations, policies, and federal laws. We'll likely don our secret decoder ring and try to untangle that surreptitious web in the future.

But for now…

When it comes to Special Access Programs, like virtually all government operations, they are mostly cumbersome bureaucratic affairs.

Though visions of a powerful shadow government of sorts may tantalize our imaginations, within the dense procedural jungle of SAPs, these programs are not inherently good or bad. Instead, SAPs are merely institutions made up of people, and like any group of people, the inner sanctums of SAPs can be comprised of good and bad individuals and good and bad ideas.

Few would competently argue against the fact that some defense programs and operations need to be tightly classified. That's not to say there aren't real concerns associated with deep black programs, very few people even know exist. Notably, the designed exclusivity and

compartmentalization of SAPs doesn't just help protect national secrets; it allows for considerably impactful information to be secured to a minute number of defense officials, legislators, and industry insiders. With such a substantial vacuum of power and influence, self-interest can easily become national interest, and suddenly SAPs can become safe houses for careless, wasteful, or even illegal activities.

Confidentiality may indeed be an unavoidable byproduct of ensuring national defense, and we cannot reasonably expect to be able to eradicate the secrecy that Special Access Programs protect. However, we can, and should, be willing to know how the underlying secrecy processes work. If for no other reason than to ensure secrecy is always maintained with a laser focus on the greater good for us all, and a reasonable balance is being maintained between the need for secrecy and the public's right to know.