DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

15 May 2015

MEMORANDUM FOR DISTRIBUTION

Subj: ACQUISITION AND USE OF COMMERCIAL CLOUD COMPUTING SERVICES

Ref: (a) Department of the Navy Chief Information Officer Memorandum, Update to Department of the Navy Approach to Cloud Computing, June 4, 2013
(b) DON CIO Memorandum, Enterprise Mobility and Cloud Service Pilot Project Governance, July 31, 2013
(c) Department of Defense CIO Memorandum, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, December 15, 2014
(d) DoD CIO Memorandum, Use of Enterprise Information Technology Standard Business Case Analysis, October 23, 2014
(e) Federal Risk Authorization and Management Program, http://cloud.cio.gov/fedramp
(f) SECNAVINST 5720.44C, Department of the Navy Public Affairs Policy and Regulations, Change Transmittal 1, October 14, 2014.
(g) DoD Cloud Computing Security Requirements Guide (SRG), v1 r1, http://iase.disa.mil/cloud_security/Pages/index.aspx
(h) DoD Instruction 8500.01, Cybersecurity, March 14, 2014

Encl: (1) Cloud Services Supplemental Guidance
(2) Revised Information Impact Levels
(3) DON Enterprise IT Abbreviated BCA

This memorandum provides updated guidance for acquiring commercial cloud services in the Department of the Navy (DON). It also cancels reference (a) and all direction concerning cloud pilots and services in reference (b).

Reference (c) states that Department of Defense (DoD) Components may now acquire cloud services directly, without employing the Defense Information Systems Agency (DISA) as a cloud broker. To ensure the consistent, best value, enterprise-wide approach directed by DoD CIO, the DON will adhere to the following requirements.

1. Each anticipated use of commercial cloud services will first be analyzed using either the DoD Enterprise IT Business Case Analysis (BCA) template provided in reference (d) or the DON Enterprise IT Abbreviated Business Case Analysis template, provided in enclosure (3). Whichever template is used, DISA- provided cloud services must be included as one of the alternatives considered. All BCAs will be reviewed by the respective Service DON Deputy CIO. Those recommended for approval will be submitted to DON CIO for final approval. Per reference (c), DON CIO will forward approved BCAs to DoD CIO.

2. Federal Risk Authorization and Management Program (FedRAMP) authorization is the minimum security baseline for all DoD commercial cloud services, as described in reference (e).

3. Non-Controlled Unclassified Information (Impact Level 2) that is publicly releasable may be hosted by a Cloud Service Provider (CSP) that is FedRAMP compliant. The decision to accept such authorization is subject to acceptance by the application/system owner, Service DON Deputy CIO, and the responsible Navy or Marine Corps Authorizing Official (AO). Level 2 information systems and applications are prime candidates for commercial cloud services due to the low attendant risk. Guidance concerning information release and public communication is provided in reference (f).

4. For more sensitive Controlled Unclassified Information (CUI) (Impact Level 4), a DoD Provisional Authorization (PA) is required in addition to FedRAMP Authorization. Per reference (g), DISA will issue a DoD PA if the CSP meets the requirements. The PA will describe the types of information and associated systems that can be hosted by a particular cloud service. The Navy or Marine Corps AO must issue an Authority to Operate accepting the risk for the system or application being hosted in a commercial cloud environment and for the environment itself.

5. A commercial cloud service hosting CUI (Impact Level 4) must be connected to customers through a cloud access point (CAP) provided by either DISA or another DoD Component. All CAPs must be approved by the DoD CIO.

6. Defense Procurement and Acquisition Policy (DPAP) will develop appropriate contract language to address the issues, guidance and requirements in DFARS Case 20 13-D024, Contracting for Cloud Services. In the interim, DON mission owners with approved BCAs are advised to use the language provided in the DPAP Class Deviation-SUBPART 239.99—CLOUD COMPUTING (DEVIATION 2015-O0011).

7. DON entities that acquire commercial cloud services are responsible for the cyberspace defense of all information and associated systems hosted therein and for ensuring that end-to-end security requirements are met in accordance with reference (h). Successful operation and defense will require collaboration and information sharing among the DON, DISA and the CSP.

The DON point of contact is Ms. Susan Shuryn, 703-695-2005; susan.shuryn@navy.mil.

John A. Zangardi
(Acting)

Distribution:
ASN RD&A
ASN M&RA

Distribution: (continued)
ASN FM&C
ASN EI&E
GC
DON/AA
DUSN (M)
DASN C4I/Space
DUSN (P)
DASN(AP)
NCCA
DNS (N4, N2/N6, N2/N6BC (DON Deputy CIO Navy)
DMCS (HQMC C4/DON Deputy CIO Marine Corps)
NAVIG
JAG
CHINFO
AUDGEN
CNR
SAPRO
NCIS
PEO EIS
FLTCYBERCOM
NAVAIRSYSCOM
NAVSEASYSCOM
SPAWARSYSCOM

CLOUD SERVICES SUPPLEMENTAL GUIDANCE

The DON is responsible for acquiring Information Technology (IT) services that meet its mission objectives and provide optimal solutions that are compliant with DoD cybersecurity requirements. The DON will:

1. Require system(s) registered in the DON variant of the DoD Information Technology Portfolio Repository (DITPR-DON) to identify any cloud service providers (CSPs) they are using and make CSP identification part of the DON Federal Information Security Management Act (FISMA) report.

2. Require that all applications are properly certified and formally approved by the appropriate Authorizing Official and that required entries are made in the DON Applications and Database Management System (DADMS).

3. Comply with DoD CIO annual IT budget guidance for cloud computing services and report all necessary information in the Select and Native Programming Data Input System- Information Technology (SNaP-IT).

4. Request connections to CSP environments for cloud security Impact Levels 4-6 through the DISA Connection Approval Office in accordance with specific commercial cloud procedures that will be published in the upcoming DoD Cloud Computing Security Requirements Guide (SRG) (reference (f)). In the interim, the DoD Information Networks (DODIN) Waiver Process should be used to obtain DoD connection approval.

5. Publish references to any processes and concepts of operation developed for DON cloud implementations. Technical components within the department are developing a managed service model to facilitate assessment, employment, and sustainment of authorized commercial cloud offerings by system and application owners. Details on the managed service provider (MSP) processes will be provided under separate cover.

REVISED INFORMATION IMPACT LEVELS

Definition: Impact Levels are defined by potential impact of an event resulting in the loss of confidentiality, integrity or availability of data, systems, or networks.

The security control baseline for all Impact Levels is predicated on moderate confidentiality and moderate integrity as defined by CNSSI 1253 and the FedRAMP Moderate Baseline. Categorize systems IAW DoDI 8510.01 and CNSSI 1253. Availability is determined by mission owner and should be specified in the contract. FedRAMP authorization is the minimum security baseline.

Level #	Maximum Data Type	Information Characterization
2	Non-Controlled Unclassified Information	Unclassified information approved for public release
		Unclassified, not designated as controlled unclassified information (CUI) or critical mission data, but requires some minimal level of access control
4	Controlled Unclassified Information	Requires protection from unauthorized disclosure as established by Executive Order 13556 (Nov 2010); Education, Training, Recruiting, Credit card information for individuals (i.e., PX or MWR events)
		PII, PHI, SSN, Credit card information for individuals, Export Control, FOUO, Law Enforcement Sensitive, Email
5	Controlled Unclassified Information + NSS	National Security Systems and other information requiring a higher level of protection as deemed necessary by the information owner, public law, or other government regulations; dedicated instance required
6	Classified up to SECRET	Pursuant to EO 12958 as amended by EO 13292; classified national security information or pursuant to the Atomic Energy Act of 1954, as amended to be Restricted Data (RD)

D E P A R T M E N T O F T H E N A V Y

Enterprise IT
Abbreviated Business Case Analysis
Version 2.0

for

<< Specify the IT Investment Here >>

<< Submittal Date >>
<< Version >>

DON Component
<< Organization >>
<< POC >>

<< IT Project Full Name >>

DON IT Enterprise Abbreviated Business Case Analysis
Approval and Change Summary

Ver. No.	Version Date	Change Purpose	Change Authority	Disposition	Reference
X.XX.XX	DD-MMM-YY	[Initial approval by ITEAA or other decision authority; change/ update to previously approved version; other]	[ITEAA or other decision authority/ governance board; integrated product team; project lead; other] <<Provide name and title>>	[Approved; approved with conditions; disapproved; cancel; other]	[Official email or memorandum] <<Provide link to document or document location>>

<<Template Instructions>>

<< Prior to submission, delete these instructions as well as all template guidance provided on the following pages>>

<<Tailor this BCA per project, given project scope, size, documentation state/availability, time, or other constraints for BCA preparation. In this example/template, Alternative 1 is described as the "Status Quo." However, if the project concerns a new requirement, adjust Alternative 1 accordingly. >>

<<This document currently provides occasional specific guidance for cloud computing, which will not apply to all BCAs. For cloud related BCAs, cost information re: DISA milCloud (a mandatory alternative) can be found at this link: https://www.milcloud.mil/capacity/estimate>>

<<Instructions regarding BCA Classification Marking:>>

<<UNCLASSIFIED: If the final BCA does not contain sensitive or classified information, mark the front and back covers "UNCLASSIFIED" (as shown on this BCA template).>>

<<FOUO: A "For Official Use Only" (FOUO) designation applies to unclassified information sensitive in nature and exempt from public release under the Freedom of Information Act. If the BCA contains such information, "FOUO" must appear on the front and back covers (where UNCLASSIFIED now appears) and on the page(s) on which the sensitive information exists.>>

<<CLASSIFIED: BCAs containing any CLASSIFIED information are to be handled through separate channels, in accordance with the submitting organization's CLASSIFIED handling process and all applicable security policy procedures.>>

CONTENTS

EXECUTIVE SUMMARY

<<Present a summary-level overview, **SHOULD NOT EXCEED 1 page.** >>

<<For example purposes, Alternative 1 is presented as a traditional, existing/status quo environment throughout this template. Adjustments should be made for new intitiatives/requirements.>>

<< If this BCA is for cloud computing, alternatives must include, at a minimum: (1) the current, status quo hosting environment; (2) the milCloud option offered by the Defense Information Systems Agency (DISA); and (3) (at least one) Commercial Cloud Service Offering (CSO) provided by [*Commercial Cloud provider*]. >>

<<For all BCAs:>>

- Summarize the current issue/requirement re: the Status Quo environment.
- Brief comparison of the Alternatives.
- How (the recommended alternative) best addresses Status Quo issue(s), e.g., generates cost savings (refer to cost table below), fully satisfies requirements, involves the least risk, etc.
- Provide a general timeframe for implementation of selected alternative, if approved: provide the projected start date and expected migration completion date by month and year.
- Provide a clear statement regarding any major operational impacts (positive and/or negative), risks, facts or assumptions that should be made known to the reviewer(s). (Refer to summary chart below)
- Include whether funding has been identified for this effort.
- (If known) Contract vehicle(s) that could be used to implement the proposed solution.

Cost Comparison of Status Quo and Alternatives Considered <<refer to Section 2.3 for details>>

	FYXX	FYXX	FYXX	FYXX	FYXX	FYXX	TOTAL
Alternative 1 (Status Quo) TOTAL Costs:							
Alternative 2 TOTAL Costs:							
Net Savings of Alt. 2:							
Alternative 3 TOTAL Costs:							
Net Savings of Alt. 3:							

Operational Benefit Summary <<refer to Section 2.5 for details; include this chart if value-added>>

Alternative	Score[(1)]	Key Points
Alternative 1 Total Score		
Alternative 2 Total Score		
Alternative 3 Total Score		

[(1)] **NOTE 1:** Operational Area scores ranged from -5 to +5. The higher the score, the greatest positive impacts

1.0 OVERVIEW

1.1 Purpose

<<Clearly state the purpose of the Business Case Analysis (BCA), including subject, to whom submitted, and any other clarifying information. For example:

This Business Case Analysis (BCA) for [name of business case] includes an objectively documented analysis, comparison of alternatives and recommendation to address [describe a critical mission need(s), requirement(s), gap(s), or problem]. It is being submitted to the [decision authority name] for review, feedback and final decision>>

1.2 Problem Statement

<<Summarize the gap/problem(s), its magnitude (i.e., which mission/functional areas, people, organizations, processes, etc. are affected) and the primary mission or business impacts if not corrected.>>

1.3 Background and Context

<<Provide additional context that explains the current situation (e.g., policy, process, environmental factors). Identify root causes (if known) and contributors to the observed problem(s). Include relevant research and information on industry or market conditions as appropriate. Keep the focus strategic.>>

1.4 Project Initiative Description and Requirement(s)

<<Provide a short, high level description of the project: what it is and what it is intended to accomplish. Address high level requirement(s), including: strategic aligment, mission needs, mandates, and functional needs. Provide key baseline value(s), overall objectives (strategic and operational) and high level timeline (start and end dates). Explain if objectives are to be achieved in increments. Appendix C may be used for detailed requirements. Specifically for cloud computing, include: Data Impact Level per the DoD Cloud Computing Security Requirements Guide (SRG), v1 r1. >>

1.5 Benefits

<<Describe the desired/expected outcomes, positive results, benefits, efficiencies, and cost savings of implementing the recommended Alternative (in measureable terms if possible).>>

1.6 Scope

<<Define the project/initiative's boundaries (e.g., technology, organizations, users, processes, functions, etc.). Explain what it includes and excludes.>>

1.7 Assumptions and Constraints

<<Briefly explain key assumptions and constraints essential to understanding the basis of the analysis contained in the business case. Include timeframe of fiscal years used in the analysis. If root causes were not identified in 1.3 because they are unknown, assumptions concerning root causes should be noted here.>>

1.8 Points of Contact and Roles & Responsibilities

<<Include contact information for: the person and organization leading the effort, the functional and technical experts and BCA developers who wrote or were consulted in the writing of the BCA, the financial person/organization who/that validated the financial measures, and other persons who may be contacted to answer questions about the BCA. Specify POC roles and responsibility in the writing of the BCA so that any questions can be more quickly addressed. A table may be used.>>

2.0 ALTERNATIVES CONSIDERED

2.1 Evaluate Possible Alternatives to the Status Quo

<<A minimum of three alternatives will be considered.>>

The following [cite number] alternatives were considered for this BCA:

- Alternative 1 – [Status Quo – name]
- Alternative 2 – [name]
- Alternative 3 – [name]

2.2 Architecture

<<If this BCA is for cloud computing, summarize the architectural environment of each Alternative. If the commercial cloud Alternative does not use the current DoD approved DON Cloud Access Point and pathway, provide an architectural drawing. If a drawing is provided, it can reside in an Appendix and referenced here. Complete this section for non-cloud BCAs only if/as applicable.>>

2.3. Cost and Estimated Savings

<<In Table 2.3, identify Alternative 1 - Status Quo costs and each additional Alternative's expected costs. Enter the savings of the alternatives considered compared to Status Quo. Identify investment decision measures/processes used (e.g., Net Present Value (NPV); Internal Rate of Return (IRR), or other (see Appendix B)). Provide the "Confidence Level" (fidelity) of each Alternative's numbers where requested. Provide a brief narrative that summarizes the data presented in the table. Also explain what budget lines are expected to increase/decrease or, if not clearly identifiable in the budget, which organization(s) will likely incur costs and which will benefit from the savings, so funding can be realigned appropriately, if needed.>>

Table 2.3 - Financial Considerations ($ in thousands)							
Alternative 1 – Status Quo	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**Total**
Investment costs							
Operations & Sustainment Costs							
TOTAL Alternative 1 Costs:							
Alternative 1 Investment Decision Measures:							
				Confidence Level = << Choose >>			
Alternative 2	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**Total**
Investment costs (Including transition costs)							
Operations & Sustainment Costs							
TOTAL Alternative 2 Costs:							
Net Savings of Alt. 2:							
Alternative 2 Investment Decision Measures:							
				Confidence Level = << Choose >>			
Alternative 3	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**FYXX**	**Total**
Investment costs (Including transition costs)							
Operations & Sustainment Costs (include SW licensing if applicable)>							
TOTAL Alternative 3 Costs:							
Net Savings of Alt. 3:							
Alternative 3 Investment Decision Measures:							
				Confidence Level = << Choose >>			

2.4 Risk Summary

<<In table 2.4, for each Alternative, identify risk probability and whether risk mitigation has been identified that could affect project/program success (e.g., dependencies on other programs, availability of funding and other resources, etc.). For each Risk Type in Table 2.4, choose either: Certain, Probable, Possible, or Improbable, as applicable, and note 'Yes or No' to whether a mitigation strategy has been identified. Also provide brief supporting narrative that summarizes each Alternative's risk assessment. Specifically address any risks noted as "Certain" or "Probable" with proposed mitigation strategy. Identify any costs associated with risk mitigation actions. Risk Summary Example: >>

Alternative [...] has an overall risk of [high, medium, low]. [Risk type] has a risk probability of "Probable" because [explain and identify possible mitigation strategy]. If such mitigation actions are taken, it is believed that the risk [could or could not] be reduced from "Probable" to an acceptable level because [explain].

Table 2.4 - Risk Considerations

ALTERNATIVE:	Alternative 1 - Status Quo		Alternative 2		Alternative 3	
RISK TYPE	**Risk Probability**	**Mitigation Identified (Y/N)**	**Risk Probability**	**Mitigation Identified (Y/N)**	**Risk Probability**	**Mitigation Identified (Y/N)**
1. Mission – Reqmts Met						
2. Cost – Remains In Scope						
3. Schedule – Attainable						
4. Sufficient Personnel (skills, etc.)						
5. Probability of Change in Reqmts						
6. Complexity Level Exceeds Projection						
7. Cybersecurity Issues						

Probability: Certain = 70 – 100%; Probable = 40 – 69%; Possible = 5 – 39%; Improbable = Near 0%

2.5 Operational Impacts

<< Definitions 1-8 below apply to Table 2.5, which is to be completed for each Alternative to show whether the Alternative has a negative (harmful) impact or a positive (beneficial) impact in each operational area listed..>>

1. **Mission/business function:** Area of business or war-fighting support the system or application falls under.
2. **Interoperability**: Should indicate number and types of interfaces needed to be operational; can also include applicable networks.
3. **Customer/User Benefit**: examples may include usability, 508 Compliance, accessibility, solution(s) for current manual processes, etc.
4. **Efficiency**: should include footprint, power and required technical personnel
5. **Cybersecurity**: if this BCA is for cloud computing, this area should answer Yes or No to: CAP, HBSS/ACAS, Encryption ability, network security, MAC Level and CAC enabled application. All should be inaccordance with the appropriate Data Security Impact Level. For other BCAs, address accordingly.
6. **Reliability/Quality**: recover within x mins, hrs, day, weeks, etc.; amount of data we can afford if any to lose?
7. **Sustainability**: Technology refresh rates, out-year costs.
8. **Other:** Can include Complexity if system is extreme in either direction (very low to very high)

After each table, clearly state the nature of any significant operational impacts the Alternative presents. Expand on significant issues, areas of concern and/or strengths and how they are likely to affect the success of the project. For example:>>

Alternative [#] had [significant, moderate, minimal, no] negative operational impacts in the areas of [list], and [significant, moderate, minimal, no] positive benefits in the areas of [list]. Speficid benefits include..... Areas of concern include....

Table 2.5 - Operational Benefits / Impacts – Alternative 1 (Status Quo)		
Operational Area	**Score[1]**	**Rationale**
1. Mission/business function		
2. Interoperability		
3. Customer/User benefit		
4. Efficiency		
5. Cybersecurity		
6. Reliability/Quality		
7. Sustainability		
8. Other		
Alternative 1 Total Score:		

[1] **NOTE 1:** Score from -5 to +5. Negative impact scores of -4 or -5 are red; high positive impact scores of +4 or +5 are green.

Table 2.5 – Operational Benefits / Impacts – Alternative 2		
Operational Area	**Score[1]**	**Rationale**
1. Mission/business function		
2. Interoperability		
3. Customer/User benefit		
4. Efficiency		
5. Cybersecurity		
6. Reliability/Quality		
7. Sustainability		
8. Other		
Alternative 1 Total Score:		

[1] **NOTE 1:** Score from -5 to +5. Negative impact scores of -4 or -5 are red; high positive impact scores of +4 or +5 are green.

Table 2.5 – Operational Benefits / Impacts – Alternative 3		
Operational Area	**Score[1]**	**Rationale**
1. Mission/business function		
2. Interoperability		
3. Customer/User benefit		
4. Efficiency		
5. Cybersecurity		
6. Reliability/Quality		
7. Sustainability		
8. Other		
Alternative 1 Total Score:		

[1] **NOTE 1:** Score from -5 to +5. Negative impact scores of -4 or -5 are red; high positive impact scores of +4 or +5 are green.

3.0 CONCLUSION

<<Identify the best option and rationale for recommended Alternative, with summary rationale data. For example:>>

After performing an analysis of the financial and non-financial benefits and risks of the alternatives, [Alternative number and name] is recommended as the most viable, best value option. It generates the greatest savings [note amount and timeframe], fully satisfies all requirements, provides the greatest operational benefits/impacts, and involves risks that, once managed, are considered acceptable.

APPENDIX A: GLOSSARY

Term	Description
Assumption	An assumption is an informed position about what is believed to be true for a situation where explicit factual knowledge is unobtainable.
Baseline	A description of the beginning condition in measureable terms and a start date from which progress can be measured.
Business Case	A fact-based argument advocating an Alternative to improve business performance results. Most are prepared to support project or acquisition investment go/no-go decisions. The project business case is not a one-time document. It provides critical information for decision making throughout the project life span.
Cloud Computing	Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware.
Constraint	Constraints are factors known or discovered that are expected to limit the analysis, possible solutions and/or expected outcomes.
Cost Savings	A reduction in costs below the projected (i.e., budgeted) level as a result of a specific initiative. Because cost savings are a reduction in the level of budgeted costs, savings are available to be recouped from the budget.
Cost Avoidance	A reduction in future unbudgeted costs that cannot be recouped from the budget.
DOTMLPF	The DOTMLPF acronym is defined by the CJCSI 3170.01G - Joint Capabilities Development System (JCIDS) as: doctrine, organization, training, materiel, leadership and education, personnel and facilities. JCIDS requires all DOTMLPF aspects (materiel and non-materiel) be considered when developing a solution/recommendation.
Investment Decision Measures	Measures that result in evaluating the financial viability of a proposal or investment. This template uses Internal Rate of Return (IRR) and Net Present Value (NPV) measures. Appendix B explains an easy approach for determining these measures.
Investment funds	Funding used for non-recurring costs to upgrade, refresh, or modernize existing systems/processes, or new developments (Economic Viability (EV) Tool Users Guide).
Internal Rate of Return (IRR)	The internal rate of return is the interest rate received for an investment consisting of discounted payments/investments (negative values) and savings achieved (positive values) that occur at regular periods.
Net Present Value (NPV)	NPV is the difference between discounted benefits and discounted costs (i.e., discounted savings/cost avoidances less discounted costs). An initiative must have an NPV > 0.0 to be considered financially viable.
Operations & Support (O&S)	All costs to sustain the system/project after it has been released to production (i.e., after deployment or upon achievement of Full Operational Capability (FOC) (Economic Viability (EV) Tool Users Guide).
Risk Management	Risk Management incudes risk management planning, identification, analysis, response planning, monitoring and control. The purpose of Risk Management is to increase the probability and impact of positive events and decrease the probability and impact of negative events.

APPENDIX B: INVESTMENT DECISION MEASURES

Example: Investing in the hypothetical scenario below and realizing the following savings each year for five years, employing a 2.2% Discount Rate, and using Microsoft Excel's NPV and IRR functions, as explained below, the below NPV and IRR values were arrived at:

- **Year 1 ($2,000,000) (initial investment)**
- Year 1: PV = $150,000 **(cost savings per year – additional investment, as applicable)**
- Year 2: PV = $450,000 "
- Year 3: PV = $600,000 "
- Year 4: PV = $650,000 "
- Year 5: PV = $670,000 "

Net Present Value (NPV): NPV is the difference between discounted benefits and discounted costs (i.e., discounted savings/cost avoidances less discounted costs). An initiative must have an NPV > 0.0 to be considered financially viable. See http://www.whitehouse.gov/omb/circulars_a094/a94_appx-c for the Nominal or Real Discount Rate. The example below uses 2.2%. **I**f your analysis uses Then-Year dollars (also known as nominal, or current dollars), use nominal discount rates. If your analysis uses constant dollars of the first year of the analysis (also known as constant, base year, or real dollars), use real discount rates.

Using Microsoft Excel NPV function, enter as follows: =NPV(A2,A3,A4,A5,A6,A7,A8). This provides a NPV of $329,182.

Internal Rate of Return (IRR): The internal rate of return is the interest rate received for an investment consisting of discounted payments/investments (negative values) and savings achieved (positive values) that occur at regular periods. The higher the IRR the more financially viable.

Using Microsoft Excel IRR function, enter as follows: =IRR(A3:A8). This provides an IRR of 7%.

	A	B
1	Data	Description
2	2.2%	Annual discount rate
3	(2,000,000)	Initial cost of investment one year from today
4	150,000	Cost savings year 1 minus additional investment, as applicable
5	450,000	Cost savings year 2 "
6	600,000	Cost savings year 3 "
7	650,000	Cost savings year 4 "
8	670,000	Cost savings year 5 "
9	Formula	Description (Result)
	=NPV(A2,A3,A4,A5,A6,A7,A8)	**NPV of this investment after five years = $329,182**
10	**=IRR(A3:A8)**	**IRR of this investment after five years = 7%**

APPENDIX C: REQUIREMENTS

<<[As applicable]>>

DEPARTMENT OF THE NAVY
ABBREVIATED BUSINESS CASE ANALYSIS