TECHNOLOGY IMPROVED CAMPUS SAFETY: WIRELESS NETWORK-BASED CAMPUS POLICE INCIDENT RESPONSE, PERSON OF INTEREST AND WITNESS IDENTIFICATION, POTENTIAL VICTIM PROTECTION, AND CONTACT TRACING

by

Patrick R. Turner

This dissertation is submitted in partial fulfillment of
requirements for the degree of

Doctor of Education

Ferris State University

May 2021

TECHNOLOGY IMPROVED CAMPUS SAFETY: WIRELESS NETWORK-BASED CAMPUS POLICE INCIDENT RESPONSE, PERSON OF INTEREST AND WITNESS IDENTIFICATION, POTENTIAL VICTIM PROTECTION, AND CONTACT TRACING

by

Patrick R. Turner

Has been approved

May 2021

APPROVED:

Tracy Ellen Russo

Tracy Ellen Russo, PhD, Chair

Steven F. Hundersmark, PhD, Member

Dan Heidt

Daniel Morgan Heidt, BS, Member

Sandra Balkema

Sandra J. Balkema, PhD, Member

Dissertation Committee

ACCEPTED:

Sandra Balkema

Sandra J Balkema, PhD, Dissertation Director
Community College Leadership Program

ABSTRACT

This product dissertation analyzes current campus safety technology use and creates a campus safety product development guide aiding campus police to drive improved incident response and campus safety. Detailed product requirements, based on law enforcement use cases and user interface layouts (a.k.a., wireframes), are modeled, leading to a high-level software development plan. The product is based on wireless network location service technology, improving campus police departments' incident response, person of interest and witness identification, potential victim protection, and contact tracing. Historical background related to technology-based campus safety is provided. Topical literature is reviewed to provide a perspective of current practices and legislation for campus safety implementation, compliance, and effectiveness. Recommendations and improvements, as extrapolated from literature, give insight into this and future direction. Conclusions are drawn with data to support the need for change to improve state of campus safety assurance.

KEY WORDS: Campus Safety, Wireless Networking, Incident Response, Campus Police Department

DEDICATION

This work is dedicated to my father who passed away January of this year. He was so excited to attend my graduation. So proud of his son. But he couldn't possibly have been prouder of me than I have been of him. I have never met a man with more integrity and more intent to walk the talk. If there is any positive thing to be said about me, it is because of my father. I am the person and man I am because of his example, his encouragement, and his chastening. He gave me my faith and my focus on "getting it done." His words ring within my ears, "Eight hours' work for eight hours' pay!" "If you don't have work to do, go home so you don't bother people who do!" He led me to believe principles such as, "If you think it can't be done, please do not bother those busy doing it!" "I don't care who is right; I just want to do what is right!" "Listen to understand, not to respond!" "You wouldn't worry so much about what other people think of you, if you realized how infrequently they, do!" And lastly, from Psalm 4:3: "But know that the LORD hath set apart him that is godly for himself: the LORD will hear when I call unto him."

Thanks Dad, I love you and miss you. This is for you!

ACKNOWLEDGMENTS

I would like to acknowledge following individuals who have supported this endeavor and my life through love, compassion, fellowship, advice, encouragement, and objective criticism. Specifically: my dissertation chair, Dr. Tracy Russo, PhD; my committee members, Dr. Steven Hundersmark, PhD, and my friend, business partner, and technical touchstone, Daniel Heidt. Laura Cullen has been my workmate for over 20 years and my sounding board for all business and life situations. My friend and mentor, Dr. Conway Jeffress, PhD, is the smartest person I know and the person who most encouraged me to challenge myself with this doctorate in community college leadership journey. He has enriched my life to such a degree that words are not enough, and so for that, I will be eternally grateful. But there is one person, without whom life would be meaningless: my wife Patty; her encouragement, but most of all, her tolerance during my moody times, times of doubt, and through times of singlemindedness, she has stood by me. Given that we have been married for 36 years during completion of this work makes her support even more special. Patty, I love you and thank you.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER ONE: INTRODUCTION

INTRODUCTION

In recent years, catastrophic campus violence has become a top critical social problem demanding a solution. Recent unprecedented events including the COVID-19 global pandemic and U. S. capitol riots threaten campus safety in ways yet unconsidered. Campus safety becomes paramount to students, their parents, society at large, politicians, educational campus administrators, staff, and faculty. Crimes ranging from active shooter, battery, hate crimes, protest/crowd incited, stalking, bullying, vandalism, and theft are rising as the news is filled with stories describing social and cultural related cyber-isolation, empathy decay, racial tension, and pandemic-related personal space awareness. Campus safety scope spans societal and cultural issues of varying significance levels and are manifested by a large number of campus safety use cases (U. S. Department of Justice: Office of Community Oriented Policing Services [COPS], 2005).

When considering current campus safety, a few things become clear. Access to technology and improved processes during a crisis is key; without reliable, real-time information, law enforcement cannot make informed decisions or execute resolution efficiently and effectively. At the University of Central Florida, an active shooter's weapon jammed, and he took his own life. First responders could not view recorded video during events because getting access to DVRs was unsafe during lockdown; it took eight hours to gain access: "We knew we were one jammed weapon away from our own [mass shooting]" (Stowell, 2018, p. 45-46). Particularly during events of extreme acts of violence involving multiple victims, perpetrators have expressed feelings of estrangement and rage and have been characterized as being disturbed. All too often, there are signs that go unnoticed because one witness does not collectively see all behaviors of an individual: “Paranoia, deep depression, self-perceived isolation, and hearing voices are all common symptoms reported by various guilty parties” (Goodman, 2009, p. 66). Minding, of course, issues of privacy, having a way to centralize information about these disparate events and behaviors allow authorities to collect, correlate, and analyze abnormalities and potentially avert crises. Improvement can be as stark as night vision goggles revealing detail previously imperceptible.

These are important caveats and are similar to tools currently used by law enforcement, ranging from data base searches to firearms. Police investigation could be greatly enhanced by improving timeliness and accuracy. Efficiently and effectively connecting disparate situational data is key to identification of those nearly located to a suspected incident (Taylor & Russell, 2012). There are most certainly many unlawful or undesirable incident use cases, like larceny of a person or vehicle, significant to this body of research. Some are summarized by Heidt and Turner (2020) that include cases as simple as locating a lost electronic device. This proposed product’s novel capabilities relate to how use of wireless network technology could potentially minimize or reduce numbers of criminal or safety related incidents on campus.

CAMPUS SAFETY VS RIGHT TO PRIVACY, THE LAW, INCIDENT RESPONSE, AND PROBABLE CAUSE

Issues regarding law enforcement's ability to keep the public safe and the public's right to privacy have always been at odds. Never has this been more apparent than today with such extreme technology advances as big data analytics and warrantless data collection on a massive scale (Segal et al., 2014; Snowden, 2019). The internet's ubiquitous availability of data, social media, wireless technology advances, facial recognition, artificial intelligence, and machine learning now provide law enforcement near-instant access to personal data previously only accessible after following well-established procedures to protect innocent. How do we reconcile use of all this technology for public safety considering various protection acts on one side —the Clery Act, Title IX, the Violence Against Women Act, and the Family Educational Rights and Privacy Act (FERPA) — and the USA Patriot Improvement and Reauthorization Act of 2006 (Patriot Act; 2006) on another, authorizing mass data mining of non-governmental databases. Right to privacy is at issue and a part of U. S. history since its beginning. Specifically, even though there is no defined U. S. Constitution article or Bill of Rights privacy amendment, the first, third, fifth, ninth, and fourteenth amendments have been interpreted by judiciary to apply to an individual's right to privacy (FindLaw, 2019; Independence Hall Association, 2020; Madison et al., 1787).

Any use of personal data must have a significant focus on individual rights requiring review of any proposed product's value and efficacy against potential issues of privacy and abuse. Technology's use of person-related data can possibly violate an individual's privacy if not managed properly. Thompson and Cole (2015) review issues related to the stored communications act considering reforming the Electronic Communications Privacy Act (ECPA) and where boundaries of data access should exist. Application of incident-response technology must be designed with similar care as law enforcement demands when using firearms. Let's explore this anecdotal comparison. All American uniformed police officers are required to carry a gun with them at all times when on duty. Whether on public patrols or taking a lunch break, their gun is safely stored within their holster; let's call this the ready mode. As soon as a police officer draws their gun from its holster, everything changes; let's call this the active mode. Rules, rights, and behavior of an officer and public around them changes between ready and active mode because of an active dangerous incident or some probable cause. Drawing of their firearm is most often dictated by a use-of-force policy. A similar distinction and change of rules can be made when using technology and our proposed product during incident response and investigation. A resulting change of rules when a gun is drawn is possible use of deadly force. Second, use of technology case creates a possible intrusion on individual privacy.

Cornell University Law School's (2021) Legal Information Institute states,

> Courts usually find probable cause when there is a reasonable basis for believing a crime may have been committed (for an arrest) or when evidence of a crime is present within a place to be searched (for a search). Under exigent circumstances, probable cause can also justify a warrantless search or seizure. (n. p.)

TECHNOLOGY AND BALANCING POLICE NEEDS TO ASSURE SAFETY VS. RIGHT TO PRIVACY

College administrators make decisions about balance continually: the balance between students' rights to effective instruction and faculty rights to academic freedom, free expression vs. hate speech, open admissions vs. completion rates. Balancing between campus safety risk vs. right to privacy threats is relevant to this study. Specifically, should administrators allow the monitoring of individuals by a system tracking people's movement, assuming probable cause exists of an alleged violent, illegal, or immoral act needs to be verified, investigated, or actively managed? This is at a time when a mere suggestion of improving this ability, which may involve innocent individuals being monitored, conjures all kinds of emotional and sometimes visceral responses due to an overarching belief that such methods will be used improperly to entrap innocents (Casella, 2003). On the other hand, people already accept the ubiquitous presence of smart phone and surveillance cameras. However, during an active shooter incident where a life or lives can be saved, this begs the question, is risk to privacy too much to ask to possibly save a life? These kinds of compromises to privacy are expanding with more safety enhancing tools, methods, and technology like traceable key card use for classroom access. The proposed product is designed mindful of these issues guided by policy.

PURPOSE OF PROPOSED CAMPUS SAFETY PRODUCT

This product research study postulates a software product filling gaps related to campus law enforcement incident response methods using a new technology-enhanced campus safety tool while attempting to balance citizenry's right to privacy. As far as is currently known, the proposed new product heretofore has not existed. This work defines and designs features, functions, and benefits of such an enterprise software solution to improve campus safety through reducing incident response time. The use and integration of campus wireless-networking location-services technology and a campus Student Information Systems (SIS) will aid Campus Police Departments with person-of-interest and/or incident witness identification, *near real time,* as well as provide more proactive measures like potential victim protection, law enforcement asset placement, and contact tracing effectively using a closed-mobile-device-network to identify and locate individual(s) near an activity or incident.

High Level Product Requirements

The proposed incident investigation tool, having continuous visibility of persons without gaps or manual handoff between sensors (e.g., cameras, officers, etc.) or bodies of information, is effective, efficient, and a deterrent to illegal or unwanted behavior on campus[1]. Important campus safety use cases define product features, functions, and benefits. A representative, although not exhaustive, list of these use cases is provided as previously described and vetted by law enforcement and college administrator interviews (Alistair, 2001; Heidt & Turner, 2020); see Appendix A. The system design must address significant administrative hurdles of implementation, including privacy assumptions within the Clery Act, the Violence Against Women Act, Title IX (discrimination based on sex), and other compliance topics and policies. The proposed system should create a demonstrative improvement between immediate identification of persons of interest and/or witnesses for a reported illegal incident and timely perpetrator apprehension/conviction. The system is expected to improve incident response and investigation timeliness and effectiveness over traditional methods such as use of cameras (footage review, facial recognition, and other camera analytics), manual canvasing, eyewitness testimony as primary evidence, ballistics analysis, fingerprints, DNA database search, Department of Motor Vehicles record search, phone, and financial records review, etc.

[1] Similar to a police body cam that is always on in a "sleep" mode, when started it goes back 20 seconds and begins to record.

Product Development, Deployment, and Performance Unknowns

The proposed product does not exist, as far as is known. Its technical design and implementation address current law enforcement technology gaps and subject technologies have not been previously similarly integrated. Therefore, topics like practical applicability to use cases and adequate system performance are open questions. Success and/or appropriateness of WI-FI use and availability of accurate building floorplans and campus maps are some unknowns only discoverable during product development and implementation. A final question is whether modern wireless technology access-points are adequate and accurate enough for location-based-analytics needed

RESEARCH PLAN AND METHOD OF PRODUCT IMPLEMENTATION

This product research study begins with a literature review of current campus safety/law enforcement methods that looks specifically at tools and methods used by law enforcement for incident response, issues of legislation, compliance, privacy, technology, and tool development. The proposed product design begins with gathering and development of product requirements to professional software development standards specifically based on Carnegie Mellon's Software Engineering Institute's Capability Maturity Model Integration (CMMI) model, level 3 methodology (CMMI Product Team, 2010). The relationships between components using a CMMI product development process flow chart include use case development (Alistair, 2001; Heidt & Turner, 2020), user interface wireframes (mock-ups), a requirements and validation plan, and more as described in Chapters Two and Three. All these are used for scope of work (SOW) development and guiding engagement with potential development partners (CMMI Development Team).

CONCLUSION

Chapter One discussed the need for a new type of campus safety enterprise software product as well as legislative, legal, cultural implications, and a high-level product description. Chapter Two provides a detailed subject literature survey relevant to Chapter One topics. Chapter Three lays out product design including high-level user interface and functional and software system and environment specifications. Chapter Four discusses methodology for product development, while Chapter Five describes high-level product implementation. Chapter Six, Conclusion, summarizes this work and provides suggestions for further study and work.

Technology may not be the only answer to improved campus safety (Casella, 2003). However, technology is well suited for collection, correlation, analysis, and timely dissemination of information to all relevant stakeholders during any critical or non-critical campus safety event. Bringing disparate pieces of information together by using algorithms to find patterns, correlate data and events, and predict trends and possible behavior may lead to future evolution of intelligence led policing (Lambert, 2010; Ulrich et al., 2020). Emerging media will continue to evolve and transform traditional crisis communication and emergency management practices (Page et al., 2013). Fusion center concepts—involving various technologies, data systems, and criminal justice agencies—opens new possibilities for intelligence led policing (Lambert, 2010) on community college campuses.

Finally, this area of research, products designed and defined for institutions of higher education (IHEs) as well as society at large, is relevant as well as timely, providing a well-needed product idea and deserving of being used by campus law enforcement and college administrators alike.

In conclusion, this research aims to define a product to reduce and avoid harm to innocents on college campuses by improving efficacy of campus police departments performing incident response while quickly investigating, resolving, and potentially avoiding dangerous or illegal incidents. Improvement to intelligence led policing and fusion center type information sharing has significant implications to this aim. Actual tool implementation would be a subsequent commercial/sponsored software development project using design specifications resulting from this dissertation.

CHAPTER TWO: LITERATURE REVIEW

INTRODUCTION

From a review of relevant literature, the availability of a campus security tool using wireless network technology to aid campus police departments with incident response, person of interest and witness identification, potential victim protection, and contact tracing does not appear to exist. Wireless network location-based services are a relatively new feature of enterprise wireless systems and appears to be mostly used for location-based marketing; thus, only scratching the surface of its potential. The following literature review provides focus on relevant categories for subject product creation. These include the current state of campus safety technology, legislation and compliance, privacy issues, law enforcement methods, incident response, data sharing, products and technology, software design, and architecture.

CURRENT STATE OF CAMPUS SAFETY TECHNOLOGY

Many articles on campus safety describe the use of technology as a boon for increased school safety on college and university campuses. These articles follow latest campus safety advancements and security technology improvements, including radios, metal detectors, scanners, closed circuit television (CCTV) surveillance systems, iris recognition, and other forms of surveillance, detection, access-control, and biometric equipment; not to mention less technical alarms, locks, and intercoms. Tech-no-security or technical security advancements have altered our public spaces, institution, and homes, creating a surveillance society, whereby security items are simultaneously ubiquitous and invisible (Casella, 2003).

Fletcher and Bryden (2007) discuss stakeholder awareness of safety services on campus as high, although utilization of such services as generally low, with the exception of security and health services use. Fletcher's study participants were dissatisfied with lighting, signage, and availability of emergency phones. Females, as a group, felt more victimized than others.

Padania et al. (2011) discusses current challenges and opportunities with cameras everywhere, intersecting human rights, video, and technology. While video presents new opportunities for freedom of expression and information, it also presents challenges and exposes vulnerabilities. These vulnerabilities relate to privacy and safety, network vulnerabilities, information overload, authentication and preservation, ethics, and policy. These vulnerabilities involve governments, tech companies, developers, investors, human rights organizations, stakeholders, and others to ensure video use is done safely, effectively, and ethically.

A report by Land and Meier (2012) concludes there are human rights project benefits realized through deployment of new technologies. New technologies can reduce costs of human rights information collection and lead to increased human rights advocacy participation. However, they also report new risks and challenges such as ensuring accuracy of collected information.

McPherson (2015) discusses the validity of video evidence and a lack of a similar level of verification performed and expected by professional journalism (metadata attached to a video such as source, place, time, and conditions of production) against rapidly expanding availability of video evidence provided by what is coined as amateur, civilian, or even accidental civilian (being at the wrong place at the wrong time with a smart phone) that produce video forms of digital evidence. Considering nationally publicized incidents, colleges now face additional federal safety laws empowering U. S. Department of Education audits of colleges (Lake, 2013).

In our current culture, a number of police agencies agree these new risks and vulnerabilities indicate anonymity is essential for encouraging citizen involvement. New anonymous messaging technology also allows picture/video attachments to be included. With camera phones' ubiquity, photo identification becomes an important adjunct to surveillance. Finally, including analytical software tools to help track tips via web-based applications can be a more effective use of agency resources.

Gilmore's (2016) dissertation describes the development of a comprehensive campus safety program at Schoolcraft College. This dissertation highlights current practices involving physical policing and use of an information operations center (IOC) used to monitor campus surveillance cameras, filtered and focused social media crawlers, and news outlet feeds; all to create a preemptive rather than reactive policing methodology. However, a scan of current campus law enforcement safety practices seems to show campus agencies are being deprived of a vital resource; namely, use of wireless network technology methods for campus safety.

LEGISLATION, COMPLIANCE, AND PRIVACY

The National Summit on Campus Public Safety executive summary states,

> The nation's academic institutions, through tradition, culture, and expectation, epitomize open and accessible nature of a free and democratic society. Currently, though, colleges and universities are among society's most vulnerable and exploitable targets for individuals and organizations seeking to cause harm and fear. (COPS, 2005, p. 3)

The summit establishes direction and recommendations to develop a national strategy for programs, information sharing, funding, and other initiatives (COPS, 2005). Bolla (2019) explores issues of assault on college and university campuses and conflicts with legislation like FERPA and Title IX. This legislation impacts effective policing of campus sexual assaults by sometimes impeding local law enforcement efforts by blocking access to student records.

Background and History

Campus safety professionals, as with general public safety, rely on general populous' many eyes; however, citizens are often reluctant to get involved, and there is a lack of tools to overcome their reticence to report suspicious activity (Goodman, 2009). The need for such public participation became very real after the unreported 1986 murder of Jeanne Clery, a student at Lehigh University, and led to passing the Student Right-to-Know and Campus Security Act of 1990. The Act mandates regular crime reporting for colleges obtaining federal student loan programs as amended by the Higher Education Amendments Act of 1998. This tool, referred to as the Clery Act, assures transparency and accountability on campuses. Since then, either voluntarily or by legislative mandate, U. S. schools have modeled change after the Campus Security Taskforce, Chancellor's Task Force on Critical Incident Management, Gubernatorial Task Force on University Campus Safety, and the Midwestern Higher Education Compact. The majority of recommended security practices lacked clear empirical validation at time of endorsement, and few have been validated inside a campus setting during intervening years (Kyle et al., 2017). Most college campuses report having appropriate emergency procedures; only 25% agree students understand them. Only 50 % of campuses indicate if a campus-wide crisis happened, all students would get a notice within five minutes, and few emphasize emergency drills or campus-wide practice (Seo et al., 2012). Up until recent years, the Clery Act, served as a focal point of federal legislation regarding campus safety.

Hites et al. (2013) describes a geospatial mixed-methods approach to assessing campus safety through use of ArcGIS geolocating database system for crime location and hot-spot analysis. Geolocating, along with surveys and interviews, sorted perceived categories of crime severity to determine whether a qualitative and quantitative correlation exists between location, crime type, and perceived safety. Finding overall correlation between perceived risk and crime incidents was not statistically significant. Similarly, Nobles et al. (2013) explore community and campus safety relative to examining the Clery Act (Student Right-to-Know, 2020) using a geospatial framework. Results illustrate important patterns of crime both on and off campus involving both students and nonstudents. Pattern types include time of day relative to liquor law violations, theft, illicit drug violations, and vandalism, listed in order of prevalence; with noise complaints and assault/battery also represented. Further, conclusions suggest incoming students would find safer housing if these predictive geospatial maps of high crime areas were made available. Maguire (2008) discuss 200 topics regarding ArcGIS, a geolocated database management system including major overviews such as geoinformatics, spatial cognition, and location-based services.

As an indication of national temperament regarding security on all educational campus, Casella (2003) says,

> The “No Child Left Behind” law, passed by President George W. Bush in 2002, provided funding for the School Security Technology Center (SSTC) at Sandia National Laboratories. Mary Green (1999), an SSTC employee, published “The Appropriate and

> Effective Use of Security Technologies in U. S. Schools" through the U. S. Department of Justice. It is considered a top-most comprehensive publications on the subject. (p. 86)

This report led to widespread adoption of security technology like implementation of technology combining a numeric PIN and a biometric palm scan to precisely identify individuals picking kids up from school (Casella, 2003), more appropriate for K-12, and didn't, at the time, lead to changes on higher education campuses. Legislative action of this nature indicates public demand for improved educational setting safety, which did not discuss on-college campus applications.

In 2013, Congress authorized funds for a new National Center for Campus Public Safety within the Department of Justice focusing on a mission of a new federal civil rights of every college student to have a reasonably safe learning environment. Historically, states were responsible for campus safety with no single, comprehensive, federal campus safety law. Only the Clery Act, which requires reporting of campus crimes, provided a means for federal government to intervene on campuses (Lake, 2013).

Campus Safety Legislation, Compliance, and Effectiveness

As the U. S. government has felt compelled to become more directly involved, safety of our schools, from nursery and day care to K-12 and higher education, legislation, oversight, and compliance related burdens have continued to be enacted.

> The relevant legislation regarding student safety on campus was born out of "The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act or Clery Act, signed in 1990, is a federal statute codified at 20 U.S.C. § 1092(f), with implementing regulations as part of the U.S. Code of Federal Regulations at 34 C.F.R. 668.46. The Clery Act requires all colleges and universities participating in federal financial aid programs to keep and disclose information about crime on and near their respective campuses. Compliance is monitored by the United States Department of Education, which can impose civil penalties, up to $35,000 per violation, against

> institutions for each infraction and can suspend institutions from participating in federal student financial aid programs. (Student Right-to-Know, 1990, n. p.)

In light of nationally publicized incidents, states have started implementing once-controversial measures influencing direction of public safety on college and university campuses. Florida Governor, Rick Scott, signed the Marjory Stoneman Douglas High School Public Safety Act on March 9, 2018. Scott said this law is a compromise but would help prevent future school shootings. The law features several controversial reforms having major implications for policies and school procedures. The law also designated $99 million for metal detectors, bulletproof glass, steel doors, and upgraded locks. The law provided $28 million for expanded mental health service teams. School boards were required to establish threat assessment teams at each school to coordinate resources, assessment, and intervention with people whose behavior may pose a threat to school safety. The law also requires schools perform active-shooter training once a semester. The law creates a voluntary program allowing non-classroom school staff members who complete 132 hours of firearm safety and proficiency training to carry guns (Winn, 2018). National Incident Management Systems (NIMS; 2010-b), Winn (2018), Mitchell and Swobodzinski, (2013); and Page et al. (2013) discuss campus safety training, and NIMS also discusses preparedness (2010-a, 2010-b). The proposed product would be valuable during threat assessment by looking at crowd formation, density, movement velocity (running), and rapid dispersal, all important indicators for deployment of law enforcement personnel.

The National Center for Campus Public Safety (2016) has summarized focus group findings of 19 public safety and compliance executives from eight institutions of higher education (IHEs) and nine professional associations. The focus group provides help so IHEs can develop a culture to manage Clery Act compliance beyond a few compliance professionals at each IHE to a more institution-wide basis.

The Handbook for Campus Safety and Security Reporting (U. S. Department of Education, Office of Post Secondary Education, 2016) discusses an institution's obligation, via the Higher Education Act of 1965 (HEA), the Crime Awareness and Campus Security Act of 1990, the Clery Act (Student Right-to-Know, 2020), and the Violence Against Women Reauthorization Act of 2013 to disclose statistics, policies, and programs related to dating violence, domestic violence, sexual assault, stalking, and more.

The new Public Safety Center, funded by Congress, was formed to articulate national standards of college safety, advance college safety standards with scientific foundations, and increase coordination among federal agencies. The intent was to shift emphasis from damages and fines to facilitating protection as well as encouraging colleges to spend more on safety and less on costly compliance efforts (Lake, 2013). Various review bodies, task forces, and professional groups have recommended additional training for campus police during critical event response using an all-hazards approach and making safety and security information widely available. Recommendations include increased foot patrols; restricting access to facilities; improved communication between campus police, faculty, and staff with mental health professionals regarding high-risk students; and instituting direct communication links between campus police and admissions, housing, and counseling (Kyle et al., 2016).

Supporting data related to importance of a wireless network-based campus safety product could be found inside the Clery Act and Title IX (U. S. Department of Education, 2020) reporting required by every campus police department (Schoolcraft College, 2019). Once proposed technology is deployed, further qualitative and/or quantitative studies can be performed to evaluate how incident prevention can be enhanced by identification and removal of potential victims from harm's way during an active, dangerous incident.

Recent Technology Related Privacy Issues

Taylor et al. (2017) review group privacy pertaining to new social and legal challenges applied to big-data analytics and other data technologies. Big data marks a fundamental technological landscape transformation, but existing norms regarding data use are proven to have little bearing on these new big-data capabilities. Broeders et al. (2017) discuss big-data analytics for national security, law enforcement, and fighting against fraud involving an emphasis shift from regulating big-data collection to regulating phases of analysis and use and giving more granular guidelines and possibilities for use enhancing industry's ability to provide safety solutions.

Stader and Williams-Cunningham (2017) discuss campus sexual assault and institutional betrayal of victims through legal constructs of Title IX. Recent Federal court verdicts serve as a warning to institutions: failing to properly respond, effectively adjudicate, protect and support potential victims, while putting public relations above student welfare, will no longer be tolerated. Ackie et al. (2020) and Anderson (2020) discuss burdens new changes to Title IX place on community colleges and universities, particularly COVID-19 pandemic crisis challenges.

CAMPUS SAFETY VS RIGHT TO PRIVACY, THE LAW, INCIDENT RESPONSE, & PROBABLE CAUSE

The proper use of technology during investigation and prevention of crime has historically rested on differences between targeted versus untargeted search as well as approved warrants vs warrantless search (Segal et al., 2014; Snowden, 2019). Segal et al. discuss concepts of an intersection warrant as a possible middle ground. They suggest accountability is an answer: “Surveillance processes must incorporate accounting mechanisms enabling all three branches of government, as well as civilian participants, to maintain and safely disclose relevant statistics on how frequently and extensively warranted-access mechanisms are used” (Segal et al., 2014, p. 3). Gursoy et al. (2016) discuss how analytics may help and Sweeney (2005) discusses an approach termed selective revelation allowing data to be shared for surveillance purposes with provable assurances of privacy protection regarding data while remaining practically useful. The following sections will explore boundaries of this issue and current right to privacy policies, laws, and legislation starting with a historical basis for a citizen’s right to privacy.

The U. S. Constitution and Amendments on Privacy

A team of researchers from FindLaw (2019) found that even though there is no specific U. S. Constitution or Bill of Rights privacy amendment(s), the first, third, fifth, ninth, and fourteenth amendments have been interpreted by judiciary to apply to an individual’s right to privacy. While the U. S. Constitution does not specifically mention right to privacy however for cases such as Roe V. Wade, the U. S. Supreme Court has found several amendments imply these rights:

- First Amendment: Provides an individual freedom to keep private their choice to practice any kind of religious belief.
- Third Amendment: Protects and individual’s home as a zone of privacy.
- Fourth Amendment: Protects right of privacy against governmental unreasonable searches and seizures.

- Fifth Amendment: Provides justification for protection of private information regarding right against self-incrimination.
- Ninth Amendment: Typically justifies privacy with a broad interpretation to protect an individual’s fundamental right to privacy; somewhat compensating for the first eight Bill of Rights amendments which do not provide such protection.
- Fourteenth Amendment: Prohibits states from making laws infringing upon personal autonomy protections provided by the first thirteen amendments. Prior to the Fourteenth Amendment, a state could make laws violating freedom of speech, religion, etc.

All of these, except the first, would appear to apply to a person’s right to privacy as it pertains to use of technology for purposes of warrantless or indiscriminate use of data or mass data collection.

The Clery Act on Privacy

The Clery Act assures transparency and accountability on campuses. It requires all colleges and universities taking advantage of federal financial aid programs to keep and disclose information about crime on and near their respective campuses.

The Handbook for Campus Safety and Security Reporting (U. S. Department of Education, Office of Post Secondary Education, 2016) discusses an institution’s obligation, via HEA, the Crime Awareness and Campus Security Act of 1990, the Clery Act, and the Violence Against Women Reauthorization Act of 2013 (VAWA) to disclose statistics, policies, and programs related to dating violence, domestic violence, sexual assault, stalking, and more.

Following are excerpts relative to privacy taken from codified law typically referred to as the Clery Act.

Title 34 (Education) CFR (Code of Federal Regulations) § 668.46 (b) Annual Security Report

> 34 CFR §[Section] 668.46 (b) (11) must include a statement of policy regarding institution's programs to prevent dating violence, domestic violence, sexual assault, and stalking, as defined in paragraph (a) and must include (ii) Procedures victims should follow, including written information about (A) The importance of preserving evidence assists those proving an alleged criminal offense occurred or may be helpful obtaining a protection order; (iii) Information about how the institution will protect the confidentiality of victims and other necessary parties, including how the institution will (A) Complete publicly available recordkeeping, including Clery Act reporting and disclosures, without inclusion of personally identifying information about the victim, see definition, section 40002(a)(20) of the Violence Against Women Act of 1994 (42 U.S.C. 13925(a)(20)); and (B) Maintain as confidential any accommodations or protective measures provided to the victim, to the extent maintaining such confidentiality would not impair institution ability to provide accommodations or protective measures.

Title 34 (Education) CFR (Code of Federal Regulations) 34 CFR § 668.46 (c) Crime Statistics

> 34 CFR § 668.46 (c) (2)(ii) states an institution may not withhold, or subsequently remove, a reported crime from its crime statistics based on a decision by a court, coroner, jury, prosecutor, or other similar non-campus official. (2)(iii) However, an institution may withhold, or subsequently remove, a reported crime from its crime statistics given rare situations where sworn or commissioned law enforcement personnel have fully investigated the reported crime and, based on results of this full investigation and evidence, have made a formal determination a given crime report is false or baseless and therefore "unfounded."

Title 34 (Education) CFR (Code of Federal Regulations) § 668.46 (h) Missing student notification policies and procedures.

> 34 CFR § 668.46 (h) (1)(iv) an institution must advise students their contact information will be registered confidentially, this information will be accessible only to authorized campus officials, and it may not be disclosed, except to law enforcement personnel to further a missing person investigation.

Title IX (Discrimination on the Basis of Sex in an Education Program) on Privacy

> Title IX of Education Amendments of 1972 is designed to eliminate (with certain exceptions) discrimination on basis of sex given any education program or activity receiving Federal financial assistance. This Title is codified under code of federal regulations, specifically CFR 34 Part 106 – Nondiscrimination on the basis of sex given education program or activates receiving federal financial assistance. This legislation does not include or address terms of: privacy, information disclosure, reporting, protection, victim, but focus' most exclusively on discriminatory behavior. This implies Title IX has little, if any, protection of a victim's or perpetrator's right to privacy.

The Violence Against Women Act on Privacy

On March 7, 2013, President Obama signed into law the Violence Against Women Reauthorization Act of 2013, or VAWA 2013. VAWA 2013 recognizes U.S. native American tribes' inherent power to exercise "special domestic violence criminal jurisdiction" over certain defendants, regardless of their Indian or non-Indian status, who commit acts of domestic violence or dating violence or violate certain protection orders in Indian country. The VAWA 2013 requires colleges to disclose statistics, policies, and programs related to dating violence, domestic violence, sexual assault, stalking, and more.

The Act modifies or expands grant conditions including requirements relating to: (1) nondisclosure of personally identifying information or other client information, (2) information sharing between grantees and subgrantees, (3) civil rights and nondiscrimination, (4) audit requirements for grants, and (5) nonprofit organizations. Specifically, (Sec. 304) amends the Higher Education Act of 1965 to expand requirements for disclosure of campus security policy and crime statistics by institutions of higher education to require education programs to: (1) promote awareness of rape and other violent sex crimes, (2) require disclosure of disciplinary proceedings involving rape and other violent sex crimes and standards of evidence governing such proceedings, and (3) establish procedures for rights of accusers and accused protection during disciplinary proceedings and confidentiality of crime victims. (Section 805) expands scope of criminal-related information which must be disclosed by a U. S. citizen petitioning for a nonimmigrant K-visa (alien fiancée or fiancé). Further research revealed this legislation does not include or address the terms *data, privacy, protection*, and deals with the terms *disclosure,* *reporting, protection, security, and victim* almost exclusively, providing personal physical security and information helpful to an individual and not protecting data.

The FERPA Act on Privacy

The FERPA Act is codified under 20 U.S.C. § 1232g; 34 CFR Part 99. These designations are read, Title 20 United States Code, section 1232, subsection g which contain the laws and what is required to be done. Title 34 Code of Federal Regulations, Part 99 are regulations and how the law is to be carried out (U. S. Department of Education, 2004, 2020).

The purpose of the relevant parts is to set requirements for protection of privacy of parents and students under section 444 General Education Provisions Act, as amended. The Act defines "directory information" as information as part of an education record of a student generally not be considered harmful or an invasion of privacy if disclosed. Section (§) 99.20 defines how a parent or eligible student can request student's education records amendment. If a parent or eligible student believes education records relating to the student contains information which is inaccurate, misleading, or violates a student's rights of privacy, they may ask educational agency or institution to amend the record.

The Patriot Act on Privacy

The Patriot Act is codified under Title VIII United States Code, which primarily governs United States immigration and citizenship. The term USA PATRIOT Act stands for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. As part of the Act of 2001, the word privacy appears only eight times and only one case mentions protection of privacy. Specifically, when speaking about State

Department’s or Immigration and Naturalization Services’ right to access criminal history of visa applicants, procedures are required before the FBI is given information access. For example, one act procedure is, “to protect any privacy rights of individuals who are subjects of such information.” The same section, regarding reporting, the act states, " the Attorney General and the Secretary of State shall jointly, consulting with the Secretary of Treasury, report to Congress describing development, implementation, efficacy, and *privacy implications of the technology standard* [emphasis added] and electronic database system described in this subsection." In other cases, privacy is used as part of titles of an agency or office, but typically using a permissive context like when defining a computer trespasser: a person who accesses a protected computer without authorization and thus *has no reasonable expectation of privacy* during any communication transmitted to, though, or from the protected computer (USA Patriot Act, 2001).

The Electronic Privacy Information Center is a Washington, DC public interest research center. EPIC, established in 1994, focuses public attention on emerging privacy and civil liberties issues while protecting information-age privacy, freedom of expression, and democratic values. EPIC’s programs and activities include policy research, public education, conferences, litigation, publications, and advocacy. EPIC’s (2020) Patriot Act analysis concluded the Act weakened numerous U. S. privacy laws, including the Cable Act subscriber privacy provisions and the Electronic Communications Privacy Act email safeguards. Therefore, the Patriot Act does very little to protect citizen’s right to privacy; factually speaking, the Patriot Act weakens citizens right to privacy, favoring pursuit of security against terrorism.

European General Data Protection Regulation and California Consumer Protection Act on Privacy

European GDPR (General Data Protection Regulation)

These recently popular public privacy regulations and legislation seek to elevate citizen's public privacy protections to a hyper-protective state. Each contain language such as, the controller shall (individual at an institution responsible for oversight of GDPR compliance), at the time when personal data are obtained, provide the data subject (the individual person who is physically present within the European Union at the time their personal data is collected) with further information necessary to ensure fair and transparent data subject's personal data processing (Intersoft Consulting, 2020):

1. The period for which the personal data will be stored, or if not possible, the criteria used to determine such a period.
2. The existence of right to request from controller access to, and rectification or erasure of personal data or restriction of processing concerning data subject or to object to processing as well as right to data portability.
3. Where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), existence of right to withdraw consent at any time, without affecting lawfulness of processing based on consent before its withdrawal.
4. The right to lodge a complaint with a supervisory authority.
5. Whether provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether data subject is obliged to provide personal data and possible consequences of failure to provide such data.
6. The existence of automated decision-making, including profiling, referred to as part of Article 22(1) and (4) and, at least as part of those cases, meaningful information about logic involved, as well as significance, and envisaged consequences of such processing for data subject.

Intersoft Consulting (2020) provides the General Data Protection Regulation (GDPR) – official legal text. The rights of data subject (individual person who is physically present within European Union at the time their personal data is collected):

1. Art. 12 Transparent information, communication, and modalities for exercise of rights for the data subject
2. Art. 13 Information to be provided where personal data are collected from the data subject
3. Art. 14 Information to be provided where personal data have not been obtained from the data subject
4. Art. 15 Right of access by the data subject
5. Art. 16 Right to rectification
6. Art. 17 Right to erasure ('right to be forgotten')
7. Art. 18 Right to restriction of processing
8. Art. 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing
9. Art. 20 Right to data portability
10. Art. 21 Right to object
11. Art. 22 Automated individual decision-making, including profiling. (Intersoft Consulting, 2020)

California Consumer Protection Act on Privacy

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California. The bill was passed by the California State Legislature and signed into law by Governor Jerry Brown on June 28, 2018, to amend Part 4 of Division 3 of the California Civil Code. Officially called AB-375, the act was introduced by Ed Chau, member of the California State Assembly, and State Senator Robert Hertzberg, and is frequently compared to the GDPR from Europe.

The CCPA gives consumers more control over personal information businesses collect about them. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared
- The right to delete personal information collected from them (with some exceptions)
- The right to opt-out of sale of their personal information
- The right to non-discrimination for exercising their CCPA rights.

Businesses with revenue of $50 million are required to give consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers who received, buy, or sell 50,000 California residents' personal information or 50% of their revenue derives from such activity. The CCPA only applies to natural persons (not entities) who are citizens even when outside of California (State of California Department of Justice, 2020).

GDPR and CCPA Applicability to this Project

The proposed product will have little opportunity to use supplemental data restricted by these types of governmental legislation beyond data collected for a campus's student information system (SIS) or enterprise resource planning (ERP) system. More importantly, such data for covered individuals would never be accessed, thus exposed, unless the individual was on campus using the campus wireless network, where and when use of such data would be justified and allowable under typical campus information technology systems acceptable use policy.

Stored Communication Act and Electronic Communication Privacy Act

Thompson and Cole (2015) review issues related to the stored communications act (SCA) considering a context of reform provided via the electronic communications privacy act (ECPA) discussing where boundaries of data access should exist regarding content of emails, private Facebook messages, YouTube videos, and so-called metadata, or noncontent information, connected to public internet transactions (e.g., websites visited, to/from and time/date stamps on emails). These acts restrict service providers voluntarily disclosing a customer's communications to government agencies or others, subject to various exceptions, while establishing government procedures requiring a provider to disclose customers' communications or records.

Probable Cause Application

Cornell University Law School's (2021) Legal Information Institute discusses a probable cause definition depends on context:

> Although the Fourth Amendment states "no warrants shall issue, but upon probable cause," it does not specify what "probable cause" actually means. The Supreme Court has attempted to clarify the meaning of the term on several occasions, while recognizing probable cause is an imprecise concept, fluid and very dependent on context. In Illinois v. Gates, the Court favored a flexible approach, viewing probable cause as a "practical, non-technical" standard calling upon "factual and practical considerations of everyday life on which reasonable and prudent men [...] act."
>
> Courts often adopt a broader, more flexible view of probable cause when alleged offenses are serious.
>
> Probable Cause Definition, Probable cause is a requirement found with the Fourth Amendment usually required before police make an arrest, conduct a search, or receive a warrant. Courts usually find probable cause when there is a reasonable basis for believing a crime may have been committed (for an arrest) or when criminal evidence is present where a searched is to be performed (for a search). Under exigent circumstances, probable cause can also justify a warrantless search or seizure. Persons

> arrested without a warrant are required to be brought before a competent authority shortly after the arrest for a prompt judicial determination of probable cause. (n. p.)

Creating Accountability and Methods for Privacy Preserving Surveillance Technology

Data collection and access to vast personally identifiable information (PII) with highly available tools and big data, is creating a privacy crisis. Privacy-preserving surveillance using selective revelation attempts to balance the need for law enforcement actionable-incident-response and investigative insight with citizenries right to privacy. Sweeney (2005) categorizes five concerns. Surveillance databases contain innocent people, courts rule persons within public spaces can have no expectation of privacy, but surveillance database info can be collected from private spaces and use of these databases violate Fair Information Practices. Exacerbating all of this is lack of judicial review or impartial oversight to weigh societal benefits against individual risks; no independent review exists limiting fishing expeditions.

Sweeney (2005) advocates technologically modelling probable cause predicate within American jurisprudence by requiring a new type of database search warrant. By maintaining database investitive value prior to meeting warrant requirements, adding protections like anonymizing identity information until probable cause can be established, then connecting them, adds value to these measures. Further efficiencies result from replacing an officer with anomaly, or data-mining, algorithms while providing informant data using various data sources. Human judges can use a combination of original-data-collector vendor contracts and software policies with regulated preset matching levels of information (person matching), creating person identifiability using minimum algorithm input. These technological measures can increase use of data, even PII data, while balancing citizen’s right to privacy.

LAW ENFORCEMENT INCIDENT RESPONSE

Schafer et al. (2010) reviewed campus-based critical incidents after Virginia Tech and Northern Illinois University shootings. Results indicated a solid base of prevention and response capacity existed; however, it still lagged behind recommended practices due to facing barriers to change.

The National Incident Management System (NIMS) (2010a, 2010b, 2010c, 2010d) is the U. S. system for managing domestic incidents, designed to be the single, comprehensive system for IHEs. IHEs are intended to implement these practices before, during, and after an emergency. The Readiness and Emergency Management for School (REM) technical assistance center (TA) presents guidance and implementation resources at no cost for IHEs. NIMS (2018) also provides a timely higher ed cybersecurity fact sheet entitled “cybersecurity considerations for institutions of higher education.”

Another valuable tool is the emerging media crisis value model (EMCVM), which provides a foundation for studying the use of social media to communicate with emergency responders during an effort to counteract public uncertainty and fear while providing timely, accurate information. Proper crisis communication protects institution reputation, increases audience activism, broadens the view of a crisis, and negates a failure to plan. Public perception of crisis handling is born out in how officials communicate with media. Controlling perception requires simple, direct, and timely information on what is occurring and what is being done to handle situations, while requiring use of social media together with traditional media. Training is available from NIMS (Page et al. 2013). NIMS (2010-b), Winn (2018), and Mitchell and

Swobodzinski (2013) also discuss campus safety training, and NIMS (2010a, 2010b) additionally discusses preparedness.

Page et al. (2013) outline the purpose and goals of crisis management and communication by defining its components and desired outcomes.

> Crisis management seeks to prevent or lessen negative outcomes of a crisis and thereby protect agencies, responders, and public. Therefore, use of social media during an emergency/crisis event can aid in:
>
> - Preparation, which involves diagnoses of vulnerabilities, selecting and training a crisis management team, to include a spokesperson, creating a crisis plan, and refine communications utilizing all media forms available
> - Response through use of mass media, Internet, and social media during preparation as well as response and recovery phases
> - Recovery while attempting to return to normal operations as soon as possible following a crisis/disaster event – also known as business continuity or continuity of operations
> - Revision involves an evaluation of responses to simulated and real crises, determining what was done right and/or wrong to better performance during a possible future disaster or crisis event. (p. 21)

In general, concepts of *perception* imply citizens acquire information through experiences that allow them to adapt their behavior and response to an event, issue, or object. This type of information gathering is known as perceptual learning. Therefore, individuals use experiences as well as information from newspapers, news broadcasts, magazines, and the internet to process crises. Social media and mobile technology increase users' feelings of empowerment, leading to a greater feeling of control over a tense situation and a willingness to help others, which could potentially mobilize crisis responders. Best practices would include seamlessly integrating multimedia messages across social media channels, timely addressing fake rumors, photos, and misinformation, and being able to determine value of a given message based on source, crisis context, and situation (Page et al., 2013).

Mendoza (2014) discusses student safety within the context of security and response time while exploring campus compliance to Title IX to keep student safe. The panel concluded administrators need to shift focus away from crisis management and more toward preventative measures and support for victims. NIMS (2010-b), Winn (2018), Mitchell and Swobodzinski (2013), and Page et al. (2013) discuss campus safety training, and NIMS (a, 2010b) discusses preparedness and preventative measures. The proposed product could support preventative measures through geospatial analysis of high crime areas looking at crowd formation, crowd density, movement velocity (running), and rapid dispersal.

LAW ENFORCEMENT METHODS

Blackwell (2019), Director of Security Solutions for Shot Spotter, states in an International Association of Campus Law Enforcement Administrators (IACLEA) report that the 2019 top five technology trends for campus safety include: IP-enabled [digital network based] cameras, mobile applications, wearable technology, gunshot detection, and facial recognition.

Police investigation includes very prescriptive and historically and culturally standard methods. These methods include incident-area canvasing, person-of-interest and witness interviews, security camera footage review, database searches such as DMV, phone records, financial records, etc. (Casella, 2003). Even with these tools, optimal law enforcement investigation requires improved timeliness, accuracy, and success when attempting to identify those who are near a suspected incident, which is almost always reported significantly after the fact. Regardless, adding yet another tool such as is being suggested, requires additional administrative resources; therefore, such a tool must demonstrate significant added value before being considered or attempting use as part of this culturally structured environment.

Becker (2005) outlines methods including forensic and legal considerations applying to specific criminal investigative techniques, an investigator's role at a crime scene, and a legal team's role prescribed by law. Procedural investigative tools for search and seizure and their impact on suspect identification, sources of information, and blood spatter are discussed. Real cases are summarized to show how results of criminal investigations play out in court.

Mitchell and Swobodzinski (2013) describe crime analysts as a vital and much-needed resource within any investigative unit where skills include data mining, social media surfing, and internet searching. A police radio call flips an analyst's role from stationary/reactive crime series identification to tactical analysis, becoming a primary intelligence center for a hot call crime or a center point for a multi-jurisdictional crime series unit. Therefore, crime analysts must have experience and skills, not to mention, tools for effective execution of these roles.

Griffin (2016) examines concerns regarding law scope governing campus safety, including the obligation of colleges and institutional liability. Areas of study included negligence claims, legislative responses to promote campus safety and impact on campus life, enterprise risk management concepts as a method of improving campus security, and institutional responses to catastrophic events, and sexual assault prevention under Title IX. All these impact roles faculty and student affairs administrators play while enhancing campus safety through information, policies, and tools for success.

Feigenbaum (2019) discusses use of data encryption as part of surveillance as it applies to law enforcement access to protect law enforcement data considering Snowden-like data breaches. The jury is out on this because encryption can cause many access problems, such as an inability to decrypt data when needed and a lack of data portability.

Examining efficacy of school safety measures related to school violence, Jennings et al. (2011) found using school resource officers (SROs), rather than law enforcement officers for dealing with problems concerning bullying, addressing racial tensions, student disrespect, and gangs is most promising for addressing problems at schools. However, serious school violence was higher within schools where security officers carried tasers and/or firearms indicating nonlethal methods are better deterrents. The study reported that of those carrying weapons, 58% carry oleoresin capsicum (pepper spray), 27% possess Tasers, and 71% carry firearms (p. 109-124). Therefore, adding crime-reducing SROs leads to a tradeoff between officer safety and program efficacy.

Crawford and Burns' (2015) findings revealed mixed and often counterintuitive results for law enforcement presence and school security efforts to control school violence. Oddly, it found adding more security guards and uniformed guards was associated with significant increases of reported serious high school violence. School metrics, such as frequency of bullying reports, daily and weekly racial tension reports, proximity to high crime area or city, gang activity, and whether 50% or more of the students felt school was important, yielded numerous statistically significant findings. All but the last metric were positive indicators to different measures of increased school violence. The metric of thinking school is important related to lower incidences of all forms of violence examined by Crawford and Burns' (2015) study.

Hites et. al. (2013) discuss geospatial relationships regarding crime types, densities, and campus safety implementation. Nobles et al. (2013) discuss geospatial relationships regarding crime and their relationship to the Clery Act implementation. The proposed product would aid geospatial analysis of crime based on a crowd formation, density, movement velocity (running), and rapid dispersal particularly near a reported incident.

Municipal police have benefited from in-car video and surveillance for decades, but campus police rarely utilize this asset as they rarely do vehicle stops. However, High Point University, High Point, NC, has been using valued-engineered, in-car video systems for five years. The investment has proven results: improved seatbelt compliance; less smoking while driving; reduced unsafe driving, moving violations, crashes involving campus vehicles: general student unruliness reduction; and safer college vehicle operation (Schumaker & Karpovich, 2018). Schumaker and Karpovich (2018) also review use of in-car video as a valuable tool for university security operations, concluding that low cost in-car video recording paired with body-worn cameras provides a near seamless record of an incident.

Casella (2003) warns that security technology has its downside, using the example of adding facial recognition technology to 3,000 cameras already within public housing that allowed authorities to run housing occupants' features through any number of crime databases. Cameras mounted on police cruisers provide a ready response to claims of brutality and other alleged offences, but they also monitor who is riding highways, at what time, and on what day. This study questioned whether this level of public scrutiny is too much and are the opportunities for abuse too great.

McPherson (2015) discusses the rigor of video evidence within professional journalism and resources for verifying validity of digitally produced evidence. For example, verification using metadata attached to a video, such as source, place, time, and conditions of production, are verification data used by professionals. This research focuses on topics of amateur- or civilian-produced digital video evidence, including even accidental civilian (being at the wrong place at the wrong time with a smart phone). These topics may inform this work's applicability locating and using civilian witnesses identified digitally through use of wireless-network location technology. The veracity and validation of their use still must bear scrutiny of verification necessary for incident response and person of interest investigation.

DATA PROTECTION AND PRIVACY

Friedewald et al. (2010) discuss emerging sciences and technologies helping to create a common framework for applying data protection and promoting industry standards. Wong et al. (2020) also discuss data protection and development of frameworks for a data protection using a commons model to overcome common data protection problems as well as a view to proper policy creation. Hamam and Derhab (2021) discuss most critical web vulnerabilities according to open web application security program Top Ten, their corresponding attacks, and their countermeasures guaranteeing protection against most severe attacks and preventing several unknown exploits. All provide enhanced privacy by protecting data.

Turner (2017) describes a portfolio of enterprise information security technology tools such as encryption of data at rest and in-flight, intrusion protection, data loss prevention, threat mitigation, and others providing a comprehensive set of technological tools used to create a multilayered enterprise security strategy for protection of enterprise systems, data, and privacy.

DATA SHARING AND THE FUSION CENTER CONCEPT

Lambert (2010) discusses a concept called Intelligence-led-policing within context of a Fusion Center related to data fusion, or data sharing. Police departments traditionally have had intelligence and information-sharing functions; however, data fusion exchanges information from different sources, including law enforcement, public safety, and private sector. When combined with analysis, data fusion can lead to actionable intelligence and data informing policy and tactical deployment of resources (p. 1-2).

Lambert (2010) explains intelligence-led policing is similar to problem-oriented policing. Intelligence-led policing refers to collaborative law enforcement—combining problem-solving policing, information sharing, and police accountability with enhanced intelligence operations. Intelligence-led policing guides policing activities toward high-frequency offenders, locations, or crimes impacting resource allocation decisions. Results from this predictive capability, combining information and efforts of two or more agencies or technologies, maximizes detecting, preventing, investigating, and responding to criminal activity.

Taylor and Russell (2012) discuss the failure of police fusion centers and national criminal intelligence sharing plan concepts which originated as a response to the September 11 attacks. The intended goal was to improve coordination of law enforcement agencies through better intelligence sharing using fusion centers where information is collected, correlated, stored, analyzed, converted into intelligence, and subsequently disseminated to other agencies. Failure was largely because the current structure and mission of law enforcement agencies and traits like autonomy and interagency ego undermine fusion centers' very essence. Initial fusion centers tended to force state and local police to use roles, strategies, and techniques inherent to military, creating potential for civil liberty abuses through combatant-like invasions of privacy and racial profiling. The proposed product includes an auditing feature to discourage this behavior.

The University of Central Florida (UCF) described common problems with aged campus video surveillance systems such as disparate recording resolution, frame rate, duration, or video footage retention. Additionally, current door access-control systems blocked first responders from accessing needed areas to view video within a timely manner. Subsequently, UCF, collaborating with experts and campus IT, installed a new centralized hyperconverged video surveillance system from Pivot3 and an upgraded access-control system allowing officers access to a new UCF global security operations center to track persons of interest across campus without moving between disparate systems. This was not possible with previous systems. UCF is also integrating access-control data with human resources processes to update room access privileges during provisioning and de-provisioning of employees tied to academic semesters, terminations, and other conditions. UCF also plans to expand use of drones for a real-time and post-event surveillance, which were a major asset to the school during two recent hurricanes. Drone images, combined with cameras and access-control data, provided a holistic view of how situations were affecting campus. Finally, mass notification systems kept students safe and informed during events (Stowell, 2018).

Ulrich et al. (2020) discuss their design structure matrix (DSM) seventh evolution. DSM is used for modeling and optimizing complex product systems using square matrices. These matrices represent complex product systems, processes, and personnel organization interconnectedness. This methodology is especially valuable for very large complex systems and may apply to advancing and optimizing fusion center data sharing.

PRODUCTS AND TECHNOLOGY

System and Device Data Sharing and Collaboration

Gow et al. (2009) review communication technology, emergency alerts, and more as they relate to campus safety. Integration of diverse information and communication technologies, including analog legacy systems (e.g., sirens and public address systems) and digital technologies such as email, internet, and mobile phones to enhance information cross-correlation to provide added value to investigative and response insight. All of this must be contextualized within many policy and legal considerations, as well as specific, often complex, administrative and procedural requirements.

Companies are gaining support for citizen involvement making universities, cities, and the U. S. safer. TipNow™, a mass communication tool, allows users to report suspicious activity. The product uses SMS messages to anonymously (servers assign an alphanumeric alias and encrypt messages) report suspicious activities to appropriate, predesignated officials (Goodman, 2009). As early as 2001, the president of Evolution Software, Inc. demonstrated a wearable security computer system that could be integrated into everyday life. The system included a wearable computer with voice recognition, a monocle headset, a micro-keyboard worn on your arm, and a shoulder-mounted camera, attempting to make security technology seem like a natural and harmonious part of daily life (Casella, 2003). Cameras capable of reading a license plate number from across parking lots networked to a laptop computer are viewable from police cruisers and police departments. Closed-circuit television systems include motion recording and analytic capability to predict events like a package left behind and others (Casella, 2003).

Butler and Lafreniere (2010) discuss efficacy and reaction to campus mass notification systems preferring mass notification over email. They caution, however, that input from and awareness training for students is essential.

Figueiras and Frattasi (2010) discuss mobile positioning and tracking from conventional to cooperative techniques on top of current wireless communication networks. Further, localization as part of heterogeneous and cooperative networks including positioning, basics of wireless communications for positioning, data fusion and filtering techniques, and more providing a unified topic treatment. Improved signal processing is hoped to improve location prediction accuracy; however, recent work modeling human behavior as part of wireless network use have led to promising results leading to what is called cooperative augmentation exploiting cooperation between user devices, further boosting location estimation accuracy.

Wardell and San Su (2011) look at harnessing citizens' collective power and engaging communities within their own response and recovery and claim social media has the power to revolutionize emergency response management. The potential is clear if challenges posed by response agency use guidelines, like demonstration of value and a characterization of reliability, can be overcome. Banjo (2012) examines critical roles that mobile phones play during and after a natural disaster; specifically, the 2010 Haiti earthquake. Infrastructure robustness and scalability play a big role as well as innovations within Information and Computer Technology for Development providing practical examples, like Google maps inside-building navigation innovations.

Wireless Positioning / Location Services

Kim and Kim (2012) discuss a radio frequency identification (RFID) location-sensing system for safety management applied as a means for enhancing worker's safety under a steel industry cargo crane. However, difficulty tagging subjects (possibly via ID card), distance limitations, radio frequency interference, and other issues limit its applicability.

In a doctoral dissertation from George Mason University, Oxedine (2013) discusses an analysis of volunteered geographic information for improved situational awareness during no-notice emergencies presented as a dashboard-like one-to-two-page document. A dashboard presents critical information (indicators) as in a succinct, visually appealing format for rapidly understandable reference of subject locations and more.

Vazquez-Llorente and Wall (2014) edit a review of communications technology and humanitarian delivery as they pertain to addressing challenges and opportunities for security risk management as well as exploring the potential of new tools to create a safer, more responsive operational environment for aid workers and conclude large improvement is crucial to this end.

Vanjale et al. (2014) discuss the use of RFID tags on in-store products with receivers triggering a web camera and initiating a perpetrator(s)-related SMS message to security personnel or police. Bai and Shen (2015) proposed RFID tags incorporated into student ID cards, which would also be used for student safety management systems. The card's RFID signal allows tracking of student arrival times, student motion path on campus, as well as unusual or unauthorized departure from campus, at which time an alarm/alert is sent to campus security and/or police.

Baniukevic et al. (2011) discuss location-based services including Wi-Fi, RFID, Bluetooth, and relative performance of each, favoring RFID and Bluetooth for positioning accuracy but Wi-Fi for large area coverage. Ultimately, a hybrid approach was considered optimal. Marques et al. (2012) discuss positioning accuracy using wireless methods inside multifloor building interiors and considering performance within fingerprint-based systems, concluding 3-meter accuracy is possible; however, accuracy metrics typically used masked important limitations.

Malaney (2014) discusses location-enabled security services for wireless networks. Specifically, using this method to ascertain if a requesting device is actually within proximity to a wireless network access point, so as to limit network access to those user devices actually within proximity to a legitimate and validated wireless access point node.

Ndzukula et al. (2017) discuss a Bluetooth low energy-based (BLE) system for personnel tracking. Although several technologies are available for indoor location-based use, such as Wi-Fi and ultra-wideband, Bluetooth-based location services is usually less expensive to deploy and all smartphones have ability to receive Bluetooth signals. BLE beacons placed indoors can be recognized by a mobile phone with average error of 1.8m at an update rate of higher than 0.5 seconds. However, BLE beaconing of a personal mobile device can be user-disabled and not regarded by users as essential, as is Wi-Fi, which also can be turned off.

Ilkhechi et al. (2017) discuss the use of location services on wireless networks and propose a scalable and fully decentralized location service scheme where burden of location updates and inquiry tasks is almost evenly distributed among nodes, improving resilience against individual node failures. Wang and Xue (2006) discuss a cost-minimization algorithm for fast location tracking inside mobile wireless networks and trade-offs regarding accuracy.

Contact Tracing

Wallace (2020) and Dionicio (2020) discuss the use of wireless network technology for human contact tracing where an individual's smart device is used to provide information on contact within a specified distance from a subject. Provisions can be investigated to provide reports of person(s) who comes into contact using prescribed criteria over a target time frame.

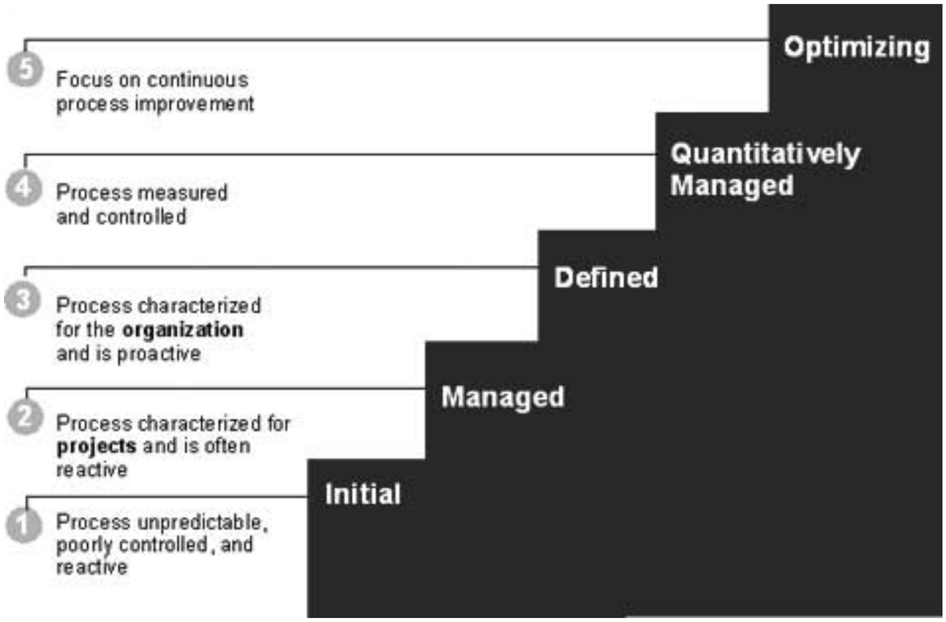
SOFTWARE DESIGN AND ARCHITECHTURE

A formal software development life cycle (SDLC) is a process whose goal is producing software with highest quality and lowest cost within a shorter timeframe. Kumar and Rashid (2018) discuss different SDLC models and their advantages and limitations while attempting to provide a systematic and disciplined understanding of activities among software engineers so quality is maintained and development time can be reduced. Chang (2001) discusses SDLC's impact on usability of software products. Mahanti et al. (2012) discuss some of the most important factors to consider when selecting a SDLC are user requirements and project complexity. CMMI follows the generally accepted seven stages of a SDLC, and this study provides a detailed set of requirements within a requirements and validation plan, and CMMI addresses our proposed product's complexity.

The Capability Maturity Model Integration (CMMI) Product Team (2010) provide a comprehensive description of Carnegie Mellon University's Software Engineering Institute's latest version of their CMMI and its use as a comprehensive, if somewhat academic, framework as an optimal SDLC. Reitzig et al. (2007) discuss CMMI-based return on investment (ROI) born out of use of CMMI methodology. Rigor of this SDLC method is sometimes thought to be enemy of other, possibly more efficient, paths to product completion and deployment. Burwick (2008), however, provides a pragmatic guide to implementation of CMMI processes, counteracting often complex and academic points of view of this global standard for software project implementation. Saeed et al. (2017) also explore, analyze, and describe the impact of CMMI regarding terms of IT industry ROI while highlighting key benefits and difficulties using CMMI compared to conventional quality assurance methodologies. The CMMI Product Team (2010) discuss SDLC as well.

The methodology chosen here for product design and development uses Carnegie Mellon University Software Engineering Institute's CMMI developed between 1987 and 1997 (White, 2021). This methodology provides highly rigorous software product design implementation processes. A software development model is used to evaluate completeness and maturity of development processes used by software development organizations, both big and small. The CMMI system has a certification process defining five levels of maturity a development organization can attain (Figure 1).

Figure 1: CMMI Maturity Levels Defined


Optimizing
5 Focus on continuous process improvement
Quantitatively Managed
4 Process measured and controlled
Defined
3 Process characterized for the **organization** and is proactive
Managed
2 Process characterized for **projects** and is often reactive
Initial
1 Process unpredictable, poorly controlled, and reactive

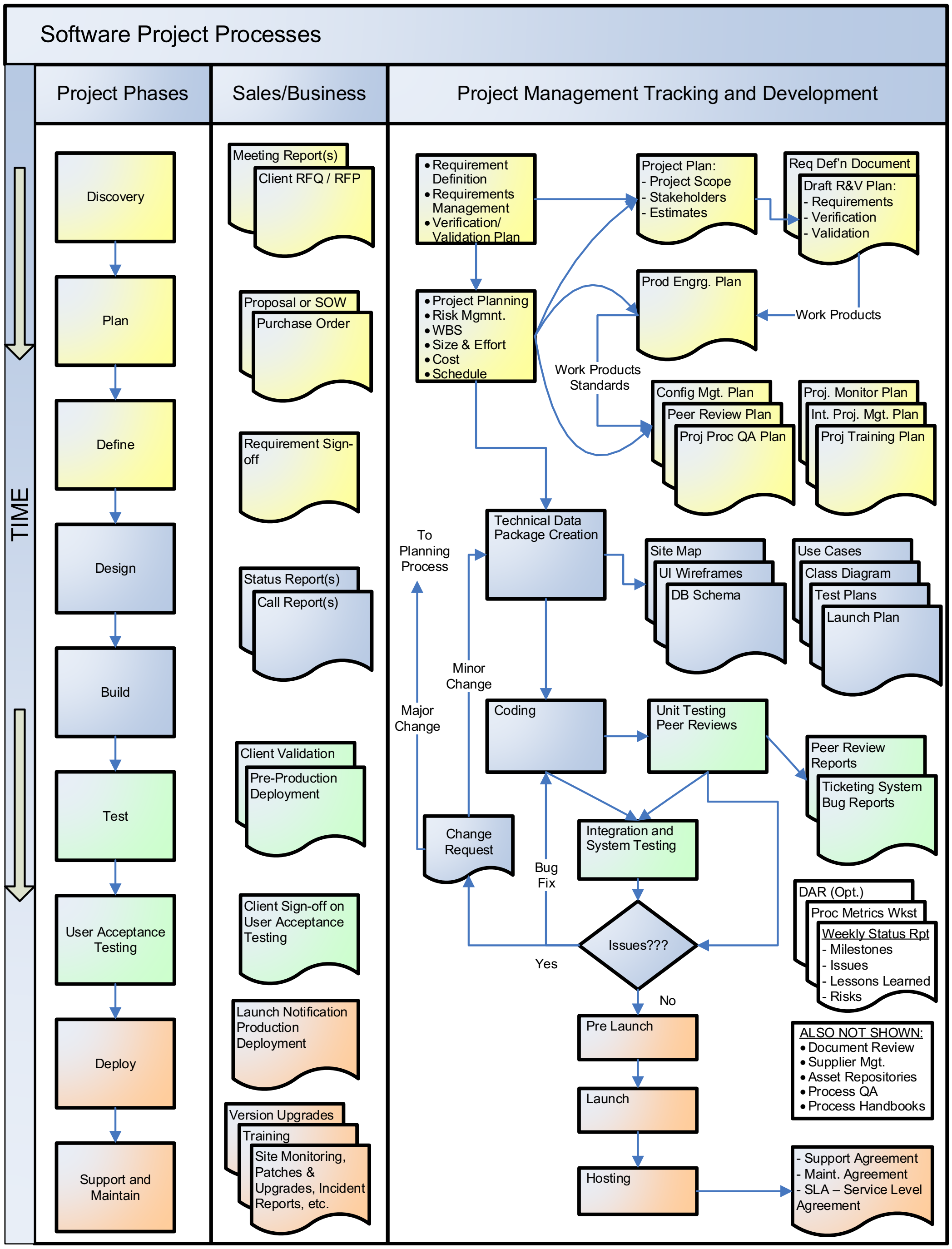
Source: White, 2021

These levels are specifically described as follows:

- Level 1 - Initial - Processes are usually ad hoc and chaotic, organizations usually do not provide a stable environment.
- Level 2 - Managed - Organizational projects ensure requirements are managed and processes are planned, performed, measured, and controlled.
- Level 3 - Defined - The organization's set of standard processes, requirements, processes, work products, and services are managed. Processes are well characterized, understood, and describe standards, procedures, tools, and methods.
- Level 4 - Quantitatively Managed - Subprocesses are selected which significantly contribute to overall process performance and subprocesses are controlled using statistical and other quantitative techniques.
- Level 5 - Optimizing - Processes are continually improved based on a quantitative understanding of common inherent causes of process variation.

Although maturity model levels are rigorous and valuable during evaluation of a development organization, it also provides a schematic for a superior development process. This product dissertation utilizes CMMI as a template for product software development. Figure 2 depicts a high-level model of this methodology aligned with typical project phases and a typical software development sales/business process.

Figure 2: Overview of CMMI Software Development Project Management Process



Vanderhyden (2018) presents tools to be used for human-centered design focusing on human elements. Optimizing usability is accomplished by including tools like cross-collaboration and implementing using human-centered design core principles, which are to empathize, define, ideate, prototype, and test when a most-valuable design occurs where desirability, feasibility, and viability intersect. Galitz (2007) provides a comprehensive introduction to graphical user interface design techniques for designing clear, easy-to-understand-and-use interfaces and screens for graphical and web systems. This eighth seminal work from a series on user-interface design topics range from knowing client, business function, and good GUI screen design principles to menus and navigation, screen controls, clear text and messages, icons, images and colors, and more.

Heidt and Turner (2020) developed a list of campus law enforcement use cases plausibly addressed by use of location technology available within enterprise wireless network systems if integrated with information available from a college campus student information systems. The use cases were vetted through interviews with law enforcement officials (Alistair, 2001). This product dissertation seeks to improve student and campus safety through use of wireless network technology to aid campus police departments with incident response, person-of-interest and witness identification, potential victim protection, and contact tracing. From Heidt and Turner's (2020) law enforcement use cases, a product idea is developed (see Appendix A). Within these use cases, all listed incidents are assumed to have happened on campus and are either in-progress or investigated after the fact:

1. Identify people within proximity to an incident or person (includes contact tracing)
2. Assault and battery
3. Destruction of property; e.g., Dumpster Fire
4. Supporting intelligence led policing (cross-discipline information sharing)
5. Larceny from building
6. Larceny from Vehicle
7. Larceny from Person

8. Criminal Sexual Conduct
9. Criminal trespass
10. Person at large shooting
11. Active Shooter
12. Location of officers for intelligent dispatch
13. Managing persons hiding during an active dangerous incident
14. Moving potential victims to safety during an active shooter or other incident
15. Monitoring and deploying tactical assets during active dangerous incident or managing massing crowds

Product development specifications begin with creation of detailed user/system requirements for features, functions, and benefits based on best practice design principles, experience constructing such products, and college law enforcement and administrator interviews. Table-top brainstorming run throughs of campus safety use cases helped refine a set of non-functional user interface wireframe designs (prototypes) and requirements rounding out a complete and comprehensive product specification (Alistair, 2001).

CONCLUSION

This chapter provided a detailed survey of literature relevant to technology-improved campus safety using wireless network-based campus police incident response, person of interest and witness identification, potential victim protection, and contact tracing.

CHAPTER THREE: METHODOLOGY – PRODUCT SPECIFICATION

INTRODUCTION

The suggested product is a web-based campus safety (Casella, 2003; Green, 1999; Griffin, 2016; Kyle et al., 2017; Lake, 2013) tool for campus police, incident response, potential victim protection, contact tracing, and more. Institutional Review Board approval was received (Appendix B). This chapter describes (a) researcher/designer- selected processes to design product content, structure, and organization; and (b) a design overview and product structure using CMMI (Burwick, 2008; CMMI Product Team, 2010; Malaney, 2014; Page et al., 2013; Reitzig et al., 2007; Saeed et al., 2017). The following chapters will present summary descriptions of tools, tests, and resources needed to implement, deploy, and train users (NIMS 2010b; Page et al., 2013; Winn, 2018) regarding product use against targeted use cases (Heidt &Turner, 2020). These use cases define products using prototyped screen shots and graphics, also called wireframes, as a guide for development (Alistair, 2001).

GOAL 1: USE CASE, USER INTERFACE, AND PRODUCT REQUIREMENTS DEVELOPMENT

This section discusses the proposed product software development framework called CMMI (CMMI Product Team, 2010), and how CMMI processes are applied for use case, user interface, and product requirements development (see Figure 2). These process outcomes provide sufficient product specification details to aid formulation of a future software development vendor request for proposal (RFP). Relative importance of RFP responses is discussed as a predictor of successful commercial product completion.

Use Case Development Process

The CMMI Product Team (2010) discusses concepts of use cases within the context of a technical solution (TS):

> [Scenarios are used] as operational concepts and operational sustainment, and development scenarios are used to generate use cases and quality attribute related scenarios used to refine architecture. Alistair (2001) discusses effective use case development methods. Use cases are also used as a means to evaluate architecture suitability for its intended purpose during architecture evaluations, which are conducted periodically throughout product design. (CMMI Product Team, 2010, p. 380)

For purposes of this product dissertation, each use case describes scenarios of actual end-user product use, aiding user interface and product functionality creation. It is best if use case scenarios are created by law enforcement subject matter experts (SMEs) or, even better, by those software development SMEs (SD-SMEs) who have spent sufficient time with former law enforcement SMEs, or LE-SMEs (in this case, LE-SMEs would be law enforcement personnel, or campus safety officers, who are involved with investigation, dispatch, incident response, and so on) to be competent writing use cases. The latter role, SD-SME, will write use cases more easily and comprehensively translate them into usable user interface screens and other system related requirements not obvious to a LE-SME. These use cases are contemplated and documented with sufficient detail as to aid creation of a comprehensive set of product requirements using CMMI templates, models, and guidelines for requirement creation (Burwick, 2008).

The use cases developed (Heidt & Turner, 2020) via above processes through cooperative brainstorming between both LE-SMEs and SD-SMEs, for the proposed product include:

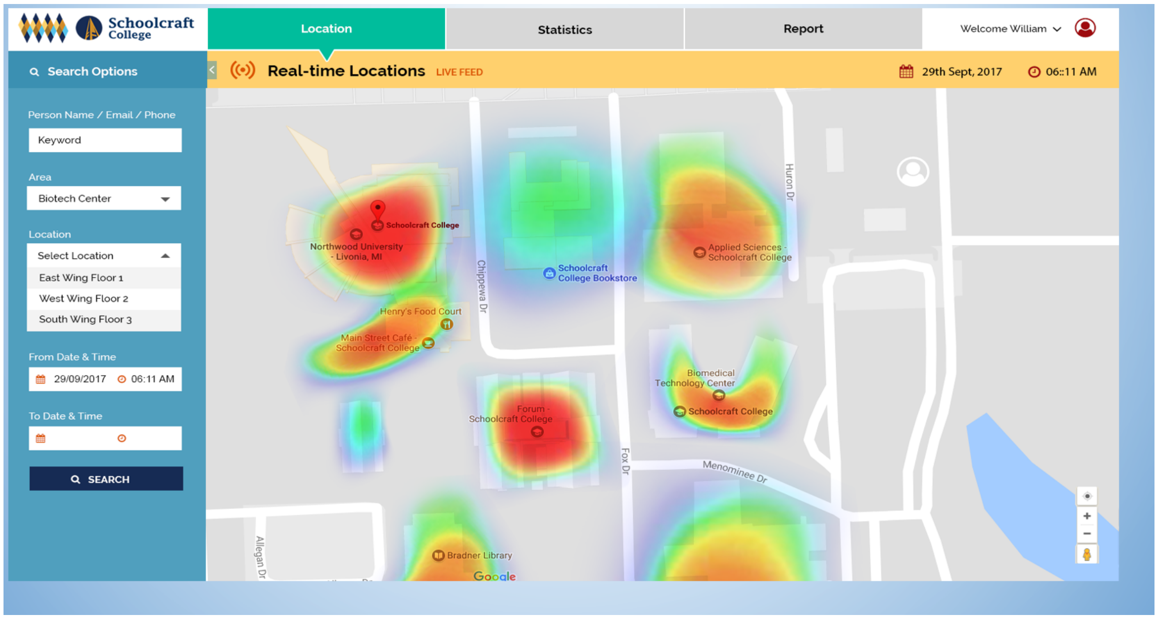
1. Active shooter (primary use case)
2. Contact tracing (primary use case)
3. Identify people within proximity of an incident
4. Assault and battery
5. Destruction of property
6. Supporting intelligence led policing
7. Larceny from building
8. Larceny from vehicle
9. Larceny from person
10. Criminal sexual conduct
11. Criminal trespass – flashlight within building, no device on third floor
12. Person at large shooting
13. Ethnic intimidation (e.g., hate crime)
14. Managing location of officers for intelligent dispatch
15. Managing persons hiding during an active dangerous incident
16. Moving potential victims to safety during an active shooter incident
17. Monitoring and deploying tactical assets during active dangerous incident or managing massing crowds
18. Investigating stalking by officer accusation

The above use cases (see Appendix A for a sample) provide a reference during table-top simulations sessions or non-functional scenario walk throughs to discuss and refine an original set of user interface wireframes (prototypes) intended to represent iterations toward layout of a final graphical user interface (GUI).

User Interface Wireframe Prototype Development

The product GUI is initially conceived via creation of wireframes, which are non-functional images of user interface screens or screen prototypes (Galitz, 2007). Figure 3 shows an example of such a proposed product wireframe. The figure image is one example of a series containing look and feel and represent contemplated proposed product GUI features. This GUI prototype is, to the best of the conceiver's ability based on their experience and expertise collaborating with various LE-SMEs and SD-SMEs, will, when fully functional, deliver needed features and functionality discussed, and assumed required for developing product use cases.

Figure 3: Example Image of a Proposed Non-functional User Interface Screen (Wireframe or GUI Prototype): Device Density Heat Map



Real-time Locations LIVE FEED 29th Sept, 2017 06::11 AM

Person Name / Email / Phone: Keyword

Area: Biotech Center

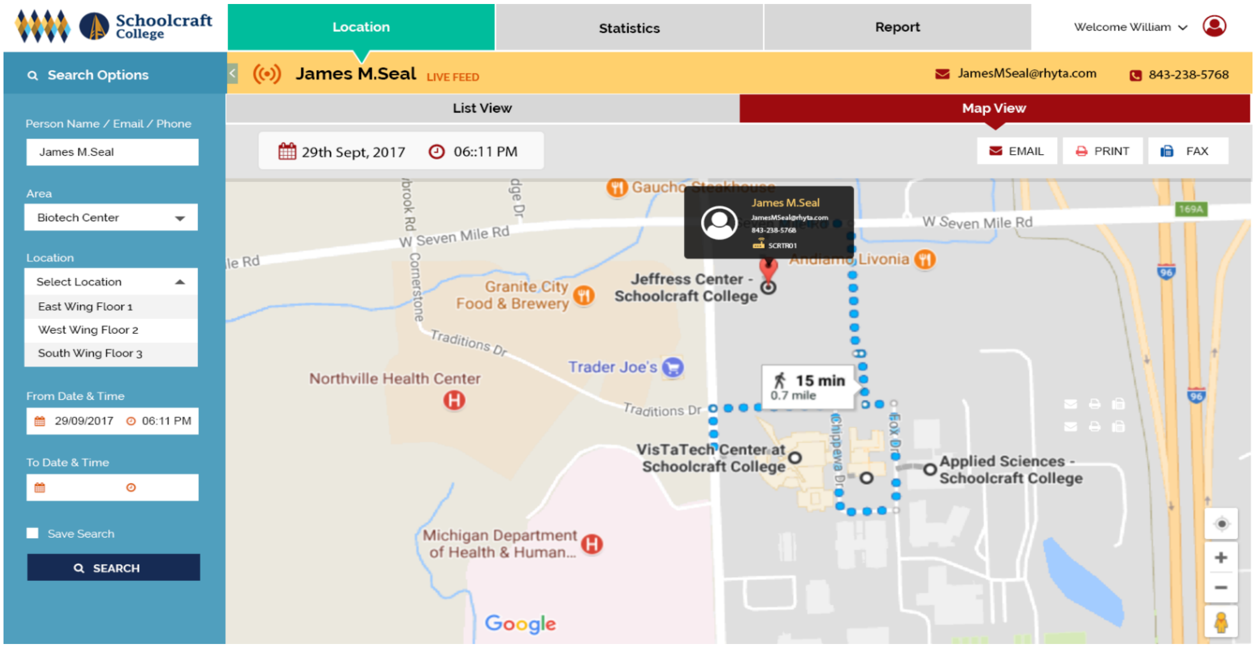
Location: Select Location

From Date & Time: 29/09/2017 06:11 AM

To Date & Time:

Figure 4 shows another sample of a user interface wireframe, which is intended to represent iterations toward layout of a full final GUI. Non-functional GUI wireframes represent best practices of user interface usability, comfortable user flow, accessibility, performance, and creation of similar types of near-real-time dashboard, monitoring, and reporting applications. Typical considerations during these walk throughs are location of widgets and features where the user would typically expect them to be, minimization of clicks to accomplish an action, immediate and understandable graphical feedback and messages, and software's reaction to user input is expected, natural and, to the extent possible, intuitive. User interface design is a vast topic, and this discussion of methodology only scratches the surface and gives directionality to steps taken to complete user interface design.

Figure 4: Campus Safety Produce User Interface Wireframes: Tracking an Individual's Location History for a Specific Time Period.



James M.Seal LIVE FEED JamesMSeal@rhyta.com 843-238-5768

29th Sept, 2017 06::11 PM

Person Name / Email / Phone: James M.Seal

Area: Biotech Center

Location: Select Location

From Date & Time: 29/09/2017 06:11 PM

To Date & Time:

Sample of Proposed Product User Interface Wireframe or Prototypes. The full plan can be provided on an as needed basis.

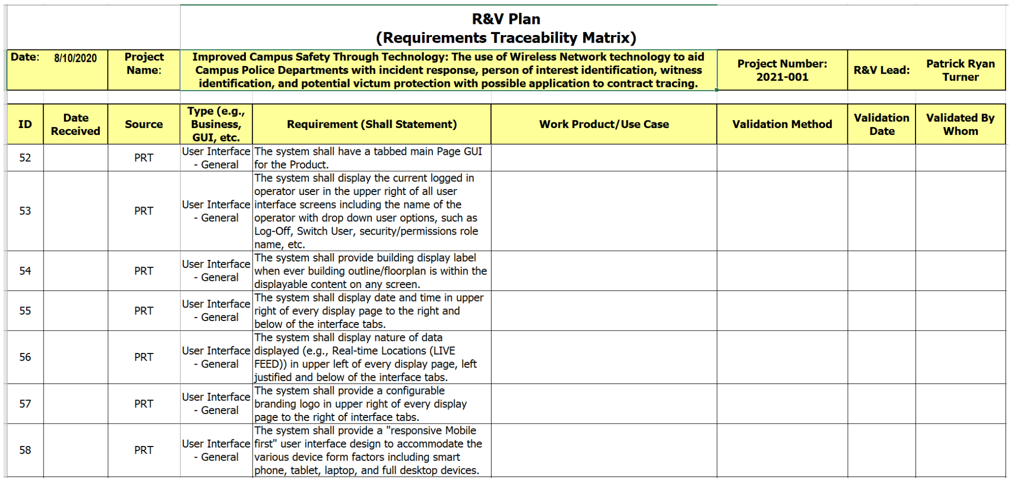
Note on Intellectual Property: The fully documented set of User Interface wireframes (Prototypes) represents researcher intellectual property and will only be provided to those involved with product commercialization.

Product Requirements: The Requirements and Validation Plan

The CMMI (2010) methodology has a very rigorous set of processes for gathering and creating product or system requirements broken into two major processes: requirements development, “to elicit, analyze, and establish customer, product, and product component requirements” (p. 325) and requirements management, “to manage requirements of project’s products and product components and to ensure alignment between those requirements and project’s plans and work products” (p. 441).

Burwick (2008) has conveniently provided a template, formally called a requirements traceability matrix combining these processes, as well as end-of-project acceptance test criteria, into a single tool called a requirements and validation plan, or R&V Plan for short. Figure 5 shows a single page example template for our proposed product.

Figure 5: Screenshot of CMMI Process Requirements Traceability Tool Sample from the Proposed Product



R&V Plan
(Requirements Traceability Matrix)

Date: 8/10/2020	Project Name:	Improved Campus Safety Through Technology: The use of Wireless Network technology to aid Campus Police Departments with incident response, person of interest identification, witness identification, and potential victum protection with possible application to contract tracing.		Project Number: 2021-001	R&V Lead:	Patrick Ryan Turner	

ID	Date Received	Source	Type (e.g., Business, GUI, etc.	Requirement (Shall Statement)	Work Product/Use Case	Validation Method	Validation Date	Validated By Whom
52		PRT	User Interface - General	The system shall have a tabbed main Page GUI for the Product.				
53		PRT	User Interface - General	The system shall display the current logged in operator user in the upper right of all user interface screens including the name of the operator with drop down user options, such as Log-Off, Switch User, security/permissions role name, etc.				
54		PRT	User Interface - General	The system shall provide building display label when ever building outline/floorplan is within the displayable content on any screen.				
55		PRT	User Interface - General	The system shall display date and time in upper right of every display page to the right and below of the interface tabs.				
56		PRT	User Interface - General	The system shall display nature of data displayed (e.g., Real-time Locations (LIVE FEED)) in upper left of every display page, left justified and below of the interface tabs.				
57		PRT	User Interface - General	The system shall provide a configurable branding logo in upper right of every display page to the right of interface tabs.				
58		PRT	User Interface - General	The system shall provide a "responsive Mobile first" user interface design to accommodate the various device form factors including smart phone, tablet, laptop, and full desktop devices.				

Source: Burwick (2008)

Burwick (2008) also provides a set of guidelines on what makes up a good set of software project guidelines. They include:

- Each requirement should be assigned an ID label to be used for traceability through testing activities.

- Keep sentences and paragraphs short.
- Use active voice.
- Use proper grammar, spelling, and punctuation.
- Use terms consistently and define them within a glossary or data dictionary.
- To see if a requirement(s) statement is sufficiently well defined, read it from a developer's perspective. Does it need additional clarification?
- Avoid long narrative paragraphs which contain multiple requirements.
- Write singular requirements so they can be easily tested.
- Avoid multiple requirements which have been aggregated into a single statement. Never use and/or as part of a requirement(s) statement as it suggests several requirements have been combined.
- Write requirements at a consistent level of detail throughout.
- Avoid redundancy.
- Begin each requirement with, "The system shall…," "The product shall...," or "The vendor shall…"

Burwick (2008) also provides a set of characteristics for what constitutes a properly formed requirement (Table 1).

The R&V plan intent is to create a comprehensive list of "shall" statements representing a desired system. Also, per Burwick's template, on each R&V plan document is a place for work products and/or use cases to be provided by potential software development vendors as part of their response to a project RFP. Here, as a part of their RFP response, proposing vendors define what part of their offered solution(s) or product(s) will satisfy each requirement with a high level of specificity. It is strongly suggested that failure to provide this information with sufficient detail (including non-responsive answers such as "complies" or "See Design Doc…") typically eliminates any further consideration of a vendor's RFP response. The next column is also filled out by potential vendors, and possibly cooperatively with a project client sponsor, to create objective, yes/no validation tests as a means to test if requirements or specifications are satisfied by as-delivered systems. Specifically, these validation tests are evaluated during or after product deployment and represent acceptance criteria for proposed solution(s) as delivered.

Table 1: Characteristics of a Properly Formed Software Requirement

PROPERTIES OF GOOD REQUIREMENTS	
Unambiguous	Ambiguity is a major problem when stating requirements. If it is not entirely clear what a system is supposed to do, it certainly cannot be tested when done.
Singular	Never use and/or within a requirement(s) statement as it suggests several requirements have been combined.
Concise (Succinct)	Requirements should deal with issues at hand and avoid rambling prose which does not contribute directly to a description of what software must do.
Non-Prescriptive	The purpose of a requirements document is to describe what software will do, not how it will do it.
Feasible	All requirements should provide a sound basis for design.
Modifiable	Good requirements are singular and testable and therefore easy to modify.
Verifiable	All requirements must be "testable."
Understandable	Requirement specifications must be understood by customers / end-users as specifications are a contract, real or informal, between customers / end-users and software developers. For a contract to be effective, customers / end-users must be able to comprehend what has been written.
Correct	A requirement(s) is defective if it is not correct. The user is sole judge of correctness. If user's intent is misrepresented, then a requirements document is not correct.
Complete	There are two ways to look at completeness of requirements. One is to determine whether any necessary requirement is missing. (It is, of course, impossible to illustrate a missing requirement without providing readers with an entire requirements document. Completeness can be thought of as one aspect of a correct requirements document as nothing user needed was omitted.) The second deals with each individual requirement. (If information is missing from requirements, a requirement itself becomes a problem.)
Precise	A requirement(s) must be stated not to be verbose and clearly describes requirements. The opposite of precise is vague (one cannot understand exactly what is being said).

PROPERTIES OF GOOD REQUIREMENTS	
Consistent	A set of requirements is inconsistent when two parts contradict each other or fail to fit together.
Traceable	Since requirements documents are to direct all subsequent software development work, it is important to be able to connect its details to subsequent document details, designs, test plans, and code. The first step of requirements traceability is to identify each document part.

Source: Burwick, 2008

Strict adherence to a requirements document is required. The R&V requirements traceability matrix is definitive as authority for all requirements. The project sponsor, at their sole discretion, will allow vendors to make requirement recommendations outside the R&V document prior to final project award; however, final approval and implementation of any of these changes is to be at sole project sponsor discretion.

The deliverables are deemed accepted upon successful completion of associated validation tests defined as part of a project R&V plan. Another consideration for this methodology is it provides a foundation for scope containment of a project by requiring a project to be fixed bid. The project sponsor needs to make very clear when time estimates are made as part of a potential vendor RFP response, such time estimates are informational only, because acceptance of all deliverables is based on successful completion of R&V plan validation tests with a positive result for each, requiring all deliverables to be complete per defined fixed bid scope. The project deliverables are a defined set of proven (validated) and accepted features per an R&V and not a bucket-of-hours. Typically, deliverables shall be accepted or rejected within five (5) consecutive business days from time of submittal for acceptance defined as validation test(s) as part of a R&V plan being executed with a positive result.

Deliverables shall be deemed accepted due to absence of review or response of acceptance within this specified time.

The project sponsor representative will determine whether a deliverable meets requirements as defined by an RFP response, or project statement of work based on successful completion of associated validation tests as part of a project R&V plan. Sometimes, added general requirements meant to catch those missing or not adequately represented by a detailed R&V plan document can be provided with this RFP for added clarity, but are only for reference.

Evaluation of a supplier’s experience implementing a proposed solution is important. The supplier must demonstrate they are capable of providing a solution that meets RFP requirements (as evaluated by validation tests within a R&V plan) and encompass flexibility, scalability, performance, management, security, and usability while leveraging project sponsor’s existing system components where feasible. Evaluation is also required of a vendor’s track record of product service, support, and customer satisfaction, as well as their commitment to developing, enhancing, and maintaining systems delivered and flexibility of systems and architecture to meet future changing business needs.

The proposed product development vendor(s) should also provide, as part of their RFP response, a system of delivered product support services, including:

1. As complete turnkey on-site implementation and project management support.
2. A toll-free customer support 24 hours per day, seven days per week.
3. An onsite training for users/technicians.
4. Future software releases and updates to all applications as part of regular software maintenance fees.

5. Technical documentation for support staff, including system overviews, design, flowcharts, and file layouts.

6. A complete set of user manuals for all software applications to document and explain system features and functions to train administrators, managers, users, and potential users (CMMI Development Team, 2010).

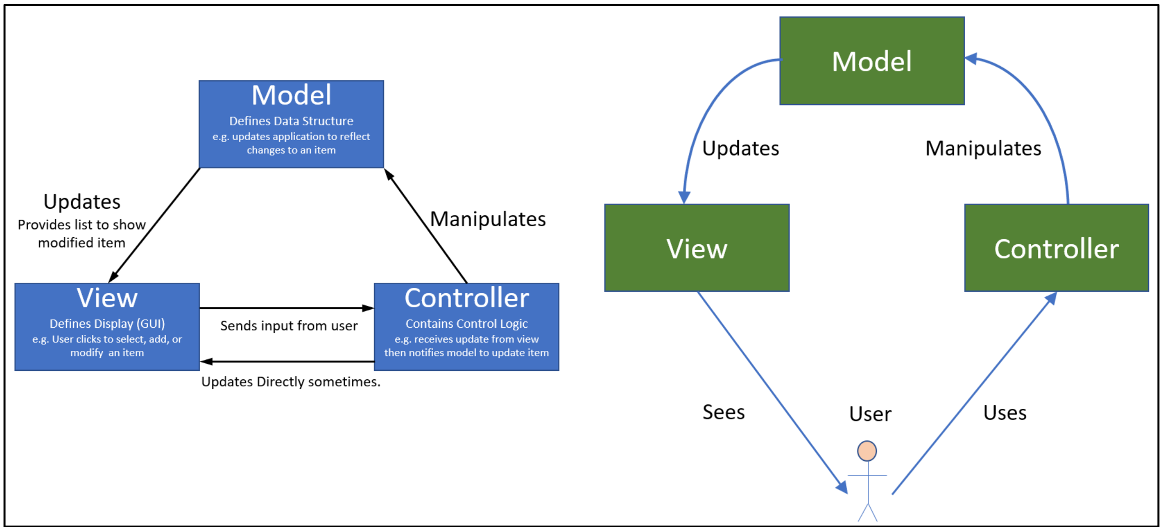
7. A proposed schedule for work based on milestones of project scope and an R&V plan (requirements and traceability matrix) included. Note: project schedule and timing is for planning and NOT for billing. Hours are not a deliverable.

GOAL 2: PRODUCT SOFTWARE ARCHITECTURE AND CMMI DEVELOPMENT PROCESS

For purposes of this product dissertation, descriptions provide sufficient detail so as to allow a competent web application development company to properly design and provide a development bid. Therefore, full CMMI model application will not be necessary for this level of specification (CMMI Development Team, 2010). The design components needed will amount to user interface wireframes (non-operational prototypes), use cases sufficient for scenario walk throughs with adequate wireframes to describe and refine final product user experience, a requirements and validation plan (R&V) providing sufficient detail to be used for final as-delivered product user acceptance testing, and a description of performance, reliability, and quality expectations as part of a service level agreement (CMMI Development Team, 2010).

The desired proposed product architecture is a three-tiered web-app architecture, also referred to as a Model, View, Controller (MVC): the model being a database schema and database management system, a view being a user interface, and a controller being an embodiment of business rules, feature implementation coding, and algorithms (logical or mathematical) used to provide product operational uniqueness. Figure 6 shows two schematic perspectives of MVC architecture.

Figure 6: Two Perspectives of MVC (Model View Controller) Software Architecture


Model
Defines Data Structure
e.g. updates application to reflect changes to an item
Updates
Provides list to show modified item
Manipulates
View
Defines Display (GUI)
e.g. User clicks to select, add, or modify an item
Sends input from user
Controller
Contains Control Logic
e.g. receives update from view then notifies model to update item
Updates Directly sometimes.
Model
Updates
Manipulates
View
Controller
Sees
User
Uses

This is a typical web-application architecture and provides benefit of being scalable, maintainable, and modifiable. It is modifiable by allowing for interchange of different subsystems, like applications programming interfaces providing support for different wireless networks or student information system manufactures.

Within our proposed software architecture design, required subsystems are as follows:

Login and Authentication

The login and authentication subsystems (Galitz, 2007) include:

1. Role-based Security: User levels include user, superuser, auditor, administrator, and system administrator roles (Refer to R&V plan for final list and role privileges).
2. Single Sign-on Integration: should be allowable as an option for proposed product ease-of-use as part of our enterprise application environment.
3. Multifactor authentication integration: should be allowable as an option for added security from unwanted or compromised product access. A secure password combined with a user specific smart phone application token confirmation method is recommended.

Geospatial Location of Network Authenticated Devices/Users

The proposed product's central capability is to provide an ability to observe a cloud of devices (smart phones, tablets, laptops, and others which authenticate and gain access to a campus wireless network) and their geospatial relationship within wireless network coverage area through location services provided by client wireless network devices, and access points (Baniukevic et al., 2011; Becker, 2005; Hites et al., 2013; Marques et al., 2012; Nobles et al., 2013).

Geospatial Location of Network Authenticated Devices

The proposed product will integrate with campus on-prem or cloud-based wireless network management system through a manufacturer provided applications programming interface (API), which provides a method of wrapping such API calls, isolating main product web-application from manufacturer specific coding for easy replacement with other suitable manufactures APIs. Specific capability of this kind will include device MAC address and user login for correlation to SIS person records, device/user location, speed, and other technical data (Baniukevic et al., 2011; Figueiras & Frattasi, 2010; Ilkhechi et al., 2017; Malaney, 2014; Marques et al. Straumsheim, 2013; 2014; Wang & Xue, 2006).

1. Access point location services: provide a user's device position through triangulation technology. It is desirable to obtain an accuracy metric from this subsystem to, for example, determine what side of a wall a device/ person is on. This should be possible with current Wi-Fi location services technology.

2. Student information system PII correlation with wireless device MAC address: Obtain SIS correlation of PII for a specific device owner or GUI-displayed person. This should be done through a suitable common database key between wireless and SIS DBMS.

3. Unregistered or unknow device handling: Display of unknown devices (i.e., persons or guests on campus but not SIS stored or for devices currently not authenticated on

a campus wireless network). Such devices are to be displayed with proper geospatial relationship to registered devices with a unique icon to distinguish them as unknown.

4. Future video surveillance time code synchronization for fusion center sharing: Provision should be provided to facilitate, but optionally implement, time code synchronization with video surveillance systems (VSS) using an industry standard format not specific to any one VSS manufacture (Casella, 2003; McPherson, 2015; Shumaker, 2018). Time code sync or similar integration would seem appropriate as a service provided by typical VSS using a NTP (Network Time Protocol) national time synchronization service server.

5. Importing building floor plans for accurate spatial positioning of device/user: A means is to be provided to import campus/building floor plans, allowing for distinction between floors of a given building, while providing capability to position and scale a building floorplan to have an accurate geo-spatial relationship within the product GIS system used; likely, Google maps.

Product Features

The main user product features are categorized as searching, tracking, contact tracing, alerting, reporting, information sharing, mobile application, and auditing as developed during table-top simulations or scenario walk throughs, using use cases documented (see Appendix A for a sample). The R&V plan provides full specification of these features. Next, general reference feature descriptions provide end users, developers, SMEs, and readers of this dissertation a context for the proposed product (Becker, 2005; Hites et al., 2013; Nobles et al., 2013).

Searching

Searching. Upon formal notification of a suspected incident to campus police once determining probable cause, or continuation of a previously properly initiated incident investigation (validated by creation or reference to one or more incident IDs and probable cause codes, or perhaps a set of questions intended to assure tool use is justified), a user technician will perform a search for a device(s)/person(s) at a reported specific location, area, or a general search to find a specific device, individual, or multiple individuals. Additionally, a user technician may perform an analysis of a specific location, area, or region to identify devices/persons within proximity to an alleged reported incident. Either of these searches can be done near real time, at a past time, or over some past interval of time. Searching past data will be limited by data retention specification, settings, or limitations of system's storage capacity. The R&V plan fully documents these user interface widgets to accomplish these features and will not be detailed here. Finally, searches can be of two types: newly initiated and saved searches. For a saved search, software inputs, filters, user interface pan and zoom settings are saved so they may be reproduced quickly. Saving screen images of a search at a given time would fall under Reporting (Becker, 2005).

Tracking

Tracking is an extrapolation of searching including path(s) a particular device/person has traveled, or is traveling, and is displayed over a user-specified past time interval accurately. This is useful for determining contact between individuals, potential witnesses to an incident, and a host of additional scenarios documented as part of product use cases. Should a search of multiple devices/individuals be done simultaneously, GUI should display a different path color. Similarly, this feature is limited to data retention issue previously discussed (Baniukevic et al., 2011; Blackwell, 2019; Figueiras & Frattasi, 2010; Ilkhechi et al., Kim & Kim, 2012; Malaney, 2014; Marques et al., 2012; Stowell, 2018; Ndzukula, 2017; Vanjale et al., 2014; Wang & Xue, 2006).

Contact Tracing

Contact tracing. The relative importance of pandemic-related contact tracing of individuals diagnosed with COVID-19 is significant. The proposed system design is capable of being used for such scenarios. Creating an algorithm that tracks a diagnosed person over a specific time should be constructed so a report of contact with others within a configurable specific distance for a settable minimum time period. The report should contain the number of contacts, the duration, and distance data. Challenges exist for such a feature related to accuracy of location services provided by a wireless access point as a central data collection sensor. Provisions should be accommodated for providing such reporting for each person who comes within a prescribed contact criterion over a target time frame (Dionicio, 2020; Wallace, 2020).

Alerting

Alerting. Provisions should be accommodated for providing active alerts for when a device/person come into wireless network coverage area(s) (whether authenticated or not). This feature allows law enforcement officials to be made aware when an individual under a duly legal restriction, or a personal protection order, barring them from being on campus nearly instantly when a restriction is violated. This provision-only specification (initial product) is due to complex privacy issues related to not wanting this system to be one of monitoring behavior, but only for incident response and/or investigation. Monitoring non-person-of-interest individuals can be viewed as a violation of privacy or stalking. Further investigation will inform legal permissibility of monitoring of such non-incident related individual such as individuals on an official sex offender list. This information might be relegated to a special report for highly privileged users or other access limiting strategies. (Casella, 2003; Broeders, et al., 2017; Goodman, 2009; Taylor et al., 2017).

Reporting

Reporting. A variety of proposed product canned report types with proper filters are desirable. They include tabular information of a person of interest's PII and location to track or apprehend them, witness PII and location for identification for questioning, potential victim PII to communicate danger avoidance instructions or send aid, a list of those within proximity to an event or incident for questioning, building or area density of persons indicating a heightened need for police presence or threshold reporting for a high crime area, and others. All reports should be exportable as an image, csv, pdf, or text files, as appropriate. The R&V plan has more detailed specification (see Figure 4). Reporting should be designed considering state and federal compliance reporting such as for Clery Act, Title IX, the VAWA, and the FERPA.

1. Ad hoc reporting. A report specification interface should be developed allowing a user to select a list of data base fields to be reported, order of those column fields, a report title (optionally including filter settings), footer with <page> of <pages> included, page orientation, and a report notes field to characterize, or display subject incident as a report footnote.

2. Saved ad hoc reports. The user should be able to save and name ad hoc reports with all settings to recall for future execution. A possible archive function could be included to save a specific execution of a report for long term evidence retention or archiving purposes since retained real-time and historic data will automatically purge after a specified time period or storage space limit is reached.

3. Reporting and sharing. A wide variety of reporting is possible which expands product applicability. Using analytics and machine learning, a system could potentially aid fusion center or data sharing activities; helping predict impact of behavior changes. For example, integration with student advising early alert systems could report situations such as a student who has not left their room for several weeks or not going to class. Such work is appropriate for future consideration after potential privacy issues have been remediated (Kyle et al., 2017; Lake, 2013; Mendoza, 2014;

NIMS, 2010a; Student Right-to-Know, 1990; Taylor & Russell, 2012; Ulrich et al., 2020).

Information or Data Sharing

Integrating this system can enhance intelligence-led policing implemented though fusion centers with a purpose of creating data fusion or data sharing expanding tactical and intelligence information for improved incident response. Police departments traditionally have sought information-sharing functions; however, data fusion exchanges from different sources, including law enforcement, public safety, and private sector, have proven difficult. Proper consideration should be given to allow easy sharing, perhaps via an application programing interface. Combining such integration with analysis, data fusion can lead to actionable intelligence informing policy and tactical deployment of resources (Lambert, 2010). Such integration should be targeted at improving intelligence-led policing by guiding police activities toward high-frequency offenders, locations, or crimes. Such predictive capability maximizes detecting, preventing, investigating, and responding to criminal activity.

As a cautionary note, failure of police fusion centers and National Criminal Intelligence Sharing Plan (NCISP) where information is collected, stored, analyzed, converted into intelligence, and subsequently disseminated failed largely because law enforcement agencies and traits like autonomy and interagency ego are counter to a fusion center's mission. A cultural shift away from state and local police using military roles, strategies, and techniques creating combatant-like responses, leading to civil liberty abuses, invasions of privacy, and racial profiling is a nontechnical requisite for success (Taylor & Russell, 2012). Encouraging a trend toward privacy preserving surveillance would provide increased hope (Sweeney, 2005).

Finally, a wide variety of complex relationships create further challenges for information sharing. Incident reporting and tracking systems built on a core premise of anonymous reporting, such as Maxient, by their design encumber free information sharing. Student information system modules, such as Ellucian's Advise may be subject to FERPA, Title IX, and other compliance related restrictions. Closed data systems, for either proprietary or compliance reasons, associated with CCTV video surveillance and many other like systems inhibit sharing. Many campus topics, such as disciplinary action subject monitoring and a host of others create nontechnical hurdles to overcome to create open and comprehensive data sharing (COPS, 2005; Feigenbaum, 2019; Gow et al., 2009; Lambert, 2010; McPherson, 2015; Stowell, 2018; Taylor et al., 2017; Taylor & Russell, 2012; Ulrich et al., 2020; U. S. Department of Education, Office of Post Secondary Education, 2016; Wardell & San Su, 2011).

Mobile Application

The proposed product partner mobile application is used to send incident-related investigation results to patrolling officers from police department command staff or dispatchers to effect tasks for incident response or investigation. Such information can contain tailored and formatted data from wireless network and SIS systems. The R&V plan has more detailed specification of features and data to be provided (see Figure 4; Banjo, 2012; Figueiras & Frattasi, 2010; Ndzukula et al., 2017; Wang & Xue, 2006). Target platforms for an initial mobile application should include Apple iOS, Android, possibly Window CE, deployable via Apple Store, Google Play Store, and others.

Use-Justification Auditing and Personal Data Protection

Search tracking initiation and other proposed product features require a system-user to provide, at a minimum, for use-auditing and use-justification assurance, the following:

1. Incident ID – new or existing Incident ID for a reported incident or furtherance of an investigation.
2. Probable cause code – or other identifying categorization or justification for proposed product use.
3. Optional questionnaire – based on the probable cause code, a more detailed set of questions may be presented before wireless and SIS data are connected to provide situational and subject visibility with proper data protection employed (Michigan Judiciary, 2021).

The above-described data provides audit information for privacy compliance and use justification and such information is only reportable to highly privileged system user roles whose job it is to monitor system use and wireless network user privacy compliance. Data protection and security methods are to be employed such as encryption of data at rest and in-flight. Equally, data anonymization for privacy preserving surveillance is also prescribed by maintaining separation between wireless network MAC address device identification and student-information-system student or user PII until probable cause is adequately established. The questionnaire may include questions similar to those found on a police search warrant application or legal subpoena, such as facts and observations establishing probable cause and/or describe property/person, suspected controlled substances, and/or behaviors to be searched or investigated (Michigan Judiciary, 2021).

Product Database Design

The proposed product database design should have appropriate performance characteristics. Given potentially vast amounts of data produced by hundreds of wireless network system access point nodes on a campus combined with possible tens of thousands of concurrent wireless devices occupying coverage areas, performance considerations while writing and reading real-time data is paramount, particularly when real-time location data is combined with relatively static data from a SIS. Data segregation and aggregation strategies need to be employed to assure product application and GUI responsiveness. The vendor shall be required to understand, have experience with, and mitigate these issues related to product database design, architecture, and schema layout. Any limitations discovered during development must be mitigated by some operational mechanisms like limited number of devices within a viewing area, aggregation of a number of devices above a threshold quantity into special screen icons, buffering, or others (Baniukevic et al., 2011; Broeders, et al. 2017; Marques et al., 2012; Taylor et al., 2017).

Business Rules/Privacy

The proposed product R&V plan contains product business rules defining its features and processes. This chapter provides a high-level description of several categories. For example, compliance rules such as Clery Act, Title IX, FERPA, and other legal requirements such as probable cause, data retention, and more are detailed as part of a R&V plan. Equally, data anonymization for privacy preserving surveillance is also prescribed by maintaining separation between wireless network MAC address device identification and student information system student or user PII until probable cause is adequately established.

CONCLUSION

The proposed product design considers input from law enforcement and software development subject matter experts assuring a product is relevant and useful and expanding capabilities of law enforcement incident response and more. This chapter provided a granular description of product features and functions needed to perform incident response tasks discussed by Heidt and Turner (2020). The next chapter will detail product development implementation using the CMMI methodology.

CHAPTER FOUR: PRODUCT DESIGN AND IMPLEMENTATION

INTRODUCTION

This chapter discusses proposed product design strategy and implementation methods.

HOW PRODUCT WAS DESIGNED

The product design is based on a need to improve campus safety incident response and provide other timely capabilities for campus law enforcement such as contact tracing. The design requires a campus setting, including a wireless network and student information system (SIS). The integration of these two requisites provides a unique opportunity to improve response to a host of use cases of interest to campus police. Researcher interview discovery engagements with law enforcement through a lens of enterprise software development experience documented relevant campus-use cases including fully described enterprise software product features. This design activity clearly captured realistic scenarios, facilitating software development scope-of-work from product feature requirements, user interface prototypes (wireframes), and a feature narrative: a complete design (Alistair, 2001).

DISCUSSION OF PRODUCT IMPLEMENTATION METHODS

The methodology for product implementation could follow any number of incarnations of software development frameworks (e.g., agile, waterfall, incremental, prototyping, spiral, star, and others) that follow a formal SDLC, defined as a process producing software with high quality, low cost, within a shorter time (Chang, 2001; CMMI Product Team, 2010; Kumar & Rashid, 2018). The CMMI process follows a SDLC framework by including seven requisite stages, generally described as:

1. Planning stage
2. Feasibility or requirements analysis stage
3. Design and prototyping stage
4. Software development stage
5. Software testing stage
6. Implementation and integration
7. Operations and maintenance

This dissertation provides information completing stages one, two, and three, as described in Chapter Three. The selected development vendor will fulfill remaining stages and will be required to comply with Carnegie Mellon's Software Engineering Institute's CMMI model; level 3 methodology (CMMI Product Team, 2010).

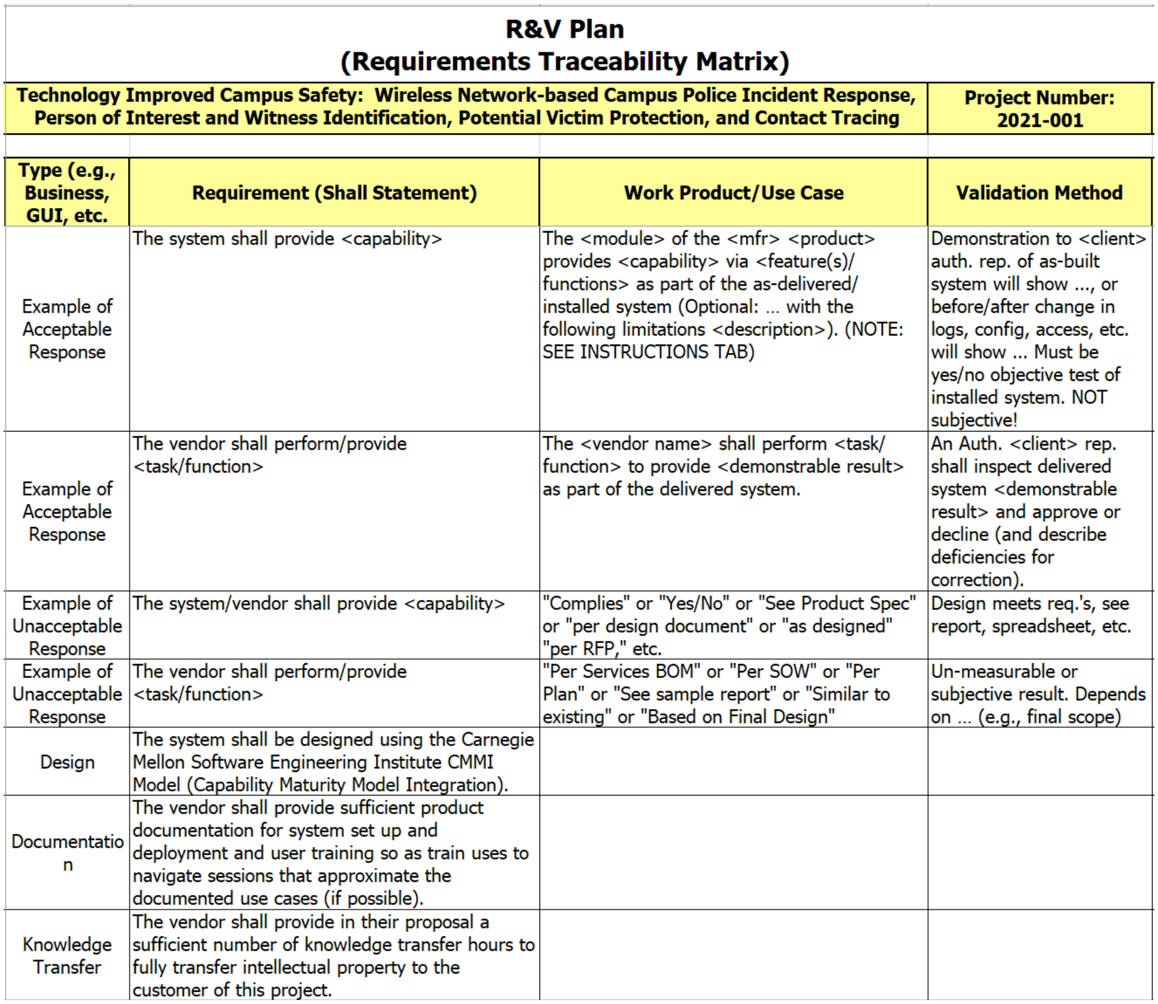
DESCRIPTION OF PRODUCT IMPLEMENTATION COMPONENTS REQUIRED

I have managed large-scale enterprise software development projects for 35 years and as a C-level executive for 25 of those years. From this experience I have developed a best practices implementation of a CMMI process framework for CMMI product development process components (see Figure 2). This framework, provided as part of this dissertation, includes use case development (Alistair, 2001; Heidt & Turner, 2020), requirements and validation plan, user interface wireframes (mock-ups), and a narrative of product functions.

The components mentioned as part of this dissertation will be used to guide an engagement with potential development partners through vendor development of an SOW (CMMI Development Team, 2010). This chapter generally describes how a potential development partner should be expected to use various CMMI methods for defining scope and managing project development processes. According to CMMI, these methods should include activities such as creating a work breakdown structure (WBS), which enumerates tasks required for project completion. The WBS is then used to estimate task size and effort that leads to a vendor quote of project cost and a development schedule with milestones including test plans, acceptance testing, deployment activities, as well as consideration of ongoing software product maintenance and support (Burwick, 2008; CMMI Development Team, 2010). Bidding software developments vendors should be expected to quote such a project as a fixed-cost engagement as a detailed R&V Plan (included), utilized properly, provides complete requirements traceability, as delivered feature validation, and a fixed set of acceptance criteria.

A software project requirements traceability matrix, comprehending a full SDLC within a single document, is captured as part of an R&V plan (see Figure 4). Figure 7 shows a sample portion of such a plan. The first column shows granular requirements first, then vendor/manufacturer responses for requirement fulfillment are documented next, and finally an as-delivered validation test, tracing a product life cycle from conception to as-delivered product acceptance. This model resists scope creep, definitively prescribes when a change request is necessary and incremental cost is justified, and provides a mutually objective measure of project completion (Burwick, 2008; CMMI Development Team, 2010).

Figure 7: Screenshot of Requirement Traceability Matrix Template with Guidance on proper Requirement Authoring



R&V Plan
(Requirements Traceability Matrix)

Technology Improved Campus Safety: Wireless Network-based Campus Police Incident Response, Person of Interest and Witness Identification, Potential Victim Protection, and Contact Tracing	Project Number: 2021-001

Type (e.g., Business, GUI, etc.	Requirement (Shall Statement)	Work Product/Use Case	Validation Method
Example of Acceptable Response	The system shall provide <capability>	The <module> of the <mfr> <product> provides <capability> via <feature(s)/ functions> as part of the as-delivered/ installed system (Optional: … with the following limitations <description>). (NOTE: SEE INSTRUCTIONS TAB)	Demonstration to <client> auth. rep. of as-built system will show ..., or before/after change in logs, config, access, etc. will show ... Must be yes/no objective test of installed system. NOT subjective!
Example of Acceptable Response	The vendor shall perform/provide <task/function>	The <vendor name> shall perform <task/ function> to provide <demonstrable result> as part of the delivered system.	An Auth. <client> rep. shall inspect delivered system <demonstrable result> and approve or decline (and describe deficiencies for correction).
Example of Unacceptable Response	The system/vendor shall provide <capability>	"Complies" or "Yes/No" or "See Product Spec" or "per design document" or "as designed" "per RFP," etc.	Design meets req.'s, see report, spreadsheet, etc.
Example of Unacceptable Response	The vendor shall perform/provide <task/function>	"Per Services BOM" or "Per SOW" or "Per Plan" or "See sample report" or "Similar to existing" or "Based on Final Design"	Un-measurable or subjective result. Depends on … (e.g., final scope)
Design	The system shall be designed using the Carnegie Mellon Software Engineering Institute CMMI Model (Capability Maturity Model Integration).		
Documentation	The vendor shall provide sufficient product documentation for system set up and deployment and user training so as train uses to navigate sessions that approximate the documented use cases (if possible).		
Knowledge Transfer	The vendor shall provide in their proposal a sufficient number of knowledge transfer hours to fully transfer intellectual property to the customer of this project.		

Sample of Proposed Product Requirements and Validations Plan; also known as a Requirements Traceability Matrix. A full plan can be provided on an as-needed basis.

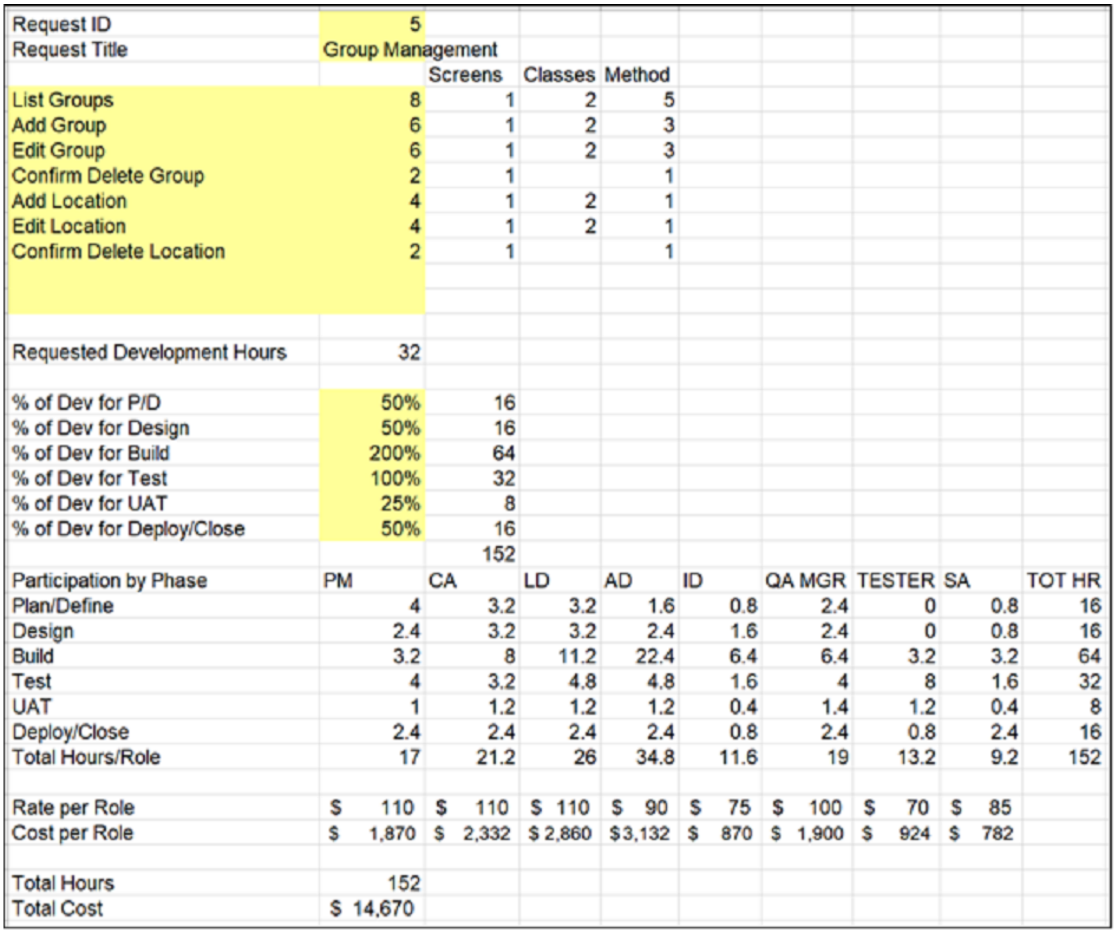
Note on Intellectual Property: The fully documented Requirements and Validation Plan (R&V Plan a.k.a. Requirements Traceability Matrix) represents researcher intellectual property and will only be provided to those involved with product commercialization.

A WBS, size and effort estimates, and cost estimation can be defined within a single tool. The WBS is a list of tasks or components needed to fulfill a request like group management. Sizes are identifiable items like screens, classes, method used to create components. Each item requires hours of effort to complete, calculating a total requested development hours. Various job description roles are required for software projects; many are non-coding-roles like project managers, testers, system admins, etc. Before costs are calculated, vendors estimate overhead per project phase. Some overhead factors exceed one 100% to include non-coding roles, multiplying them with RDH to calculate 152 actual project hours. Development cost is labor rate per role per phase. Roles include project manager (PM), chief architect (CD), lead developer (LD), associate developer (AD), interface developer (ID), systems administrator (SA), and others. Figure 8 illustrates the estimating tool.

In this example, requested total hours remain 152 for all roles, costing $14,670. This process is repeated for each major software request/component leading to total project cost. Other tools support this request estimator tool, like a controls tool that drives the third estimator tool section above by multiplying role participation percentage per phase by actual project hours so proper role rates are applied to each role's actual number of hours (Figure 9).

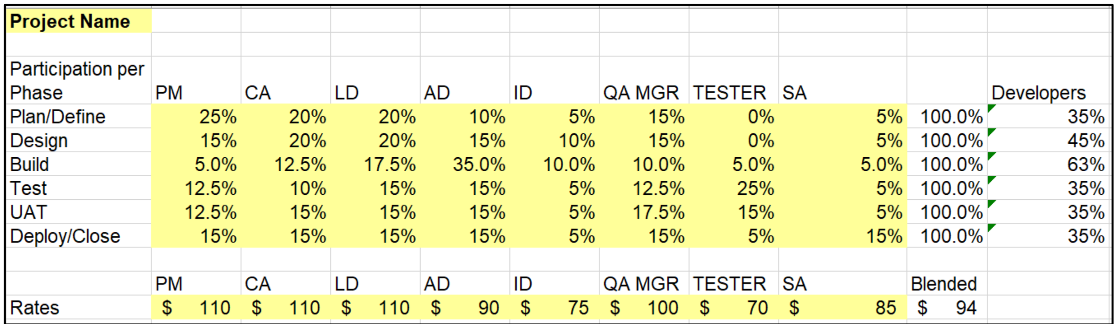
This group of tools contribute to managing project scope, cost, and development resources. The overall cost is summarized as a chart shown in Figure 10 and a schedule can be constructed and reported via a Gantt format.

Figure 8: Estimating Tool



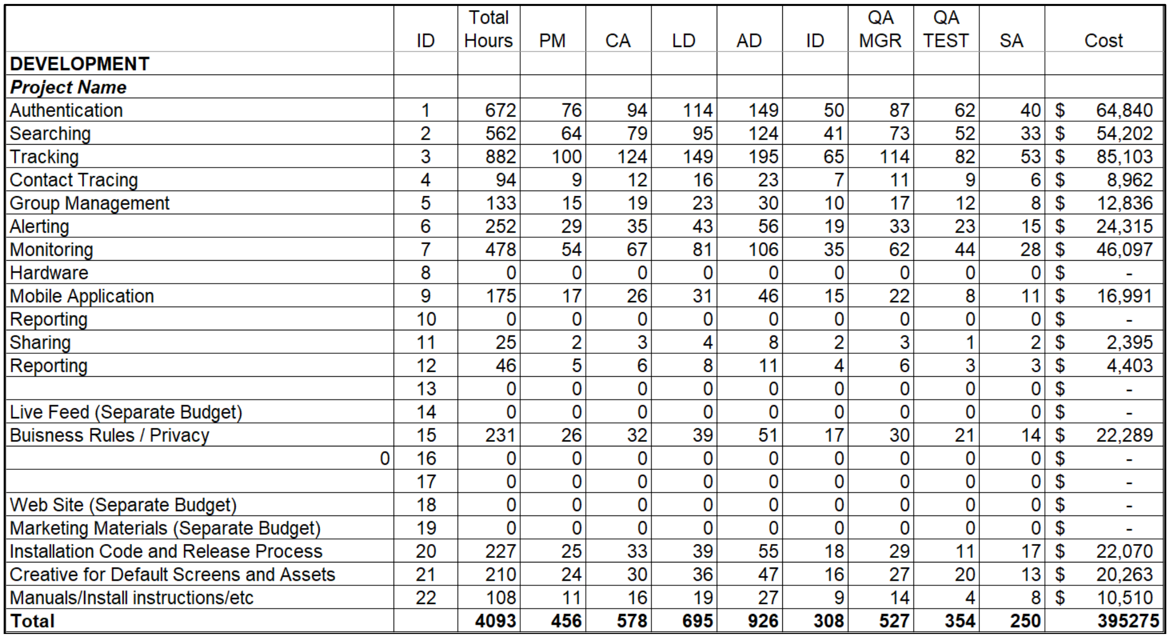
Request ID	5								
Request Title	Group Management								
		Screens	Classes	Method					
List Groups	8	1	2	5					
Add Group	6	1	2	3					
Edit Group	6	1	2	3					
Confirm Delete Group	2	1		1					
Add Location	4	1	2	1					
Edit Location	4	1	2	1					
Confirm Delete Location	2	1		1					
Requested Development Hours	32								
% of Dev for P/D	50%	16							
% of Dev for Design	50%	16							
% of Dev for Build	200%	64							
% of Dev for Test	100%	32							
% of Dev for UAT	25%	8							
% of Dev for Deploy/Close	50%	16							
		152							
Participation by Phase	PM	CA	LD	AD	ID	QA MGR	TESTER	SA	TOT HR
Plan/Define	4	3.2	3.2	1.6	0.8	2.4	0	0.8	16
Design	2.4	3.2	3.2	2.4	1.6	2.4	0	0.8	16
Build	3.2	8	11.2	22.4	6.4	6.4	3.2	3.2	64
Test	4	3.2	4.8	4.8	1.6	4	8	1.6	32
UAT	1	1.2	1.2	1.2	0.4	1.4	1.2	0.4	8
Deploy/Close	2.4	2.4	2.4	2.4	0.8	2.4	0.8	2.4	16
Total Hours/Role	17	21.2	26	34.8	11.6	19	13.2	9.2	152
Rate per Role	$ 110	$ 110	$ 110	$ 90	$ 75	$ 100	$ 70	$ 85	
Cost per Role	$ 1,870	$ 2,332	$ 2,860	$3,132	$ 870	$ 1,900	$ 924	$ 782	
Total Hours	152								
Total Cost	$ 14,670								

Figure 9: Sample Tool Used to Develop Percentage Each Role Contributes to Project Phases



Project Name										
Participation per Phase	PM	CA	LD	AD	ID	QA MGR	TESTER	SA		Developers
Plan/Define	25%	20%	20%	10%	5%	15%	0%	5%	100.0%	35%
Design	15%	20%	20%	15%	10%	15%	0%	5%	100.0%	45%
Build	5.0%	12.5%	17.5%	35.0%	10.0%	10.0%	5.0%	5.0%	100.0%	63%
Test	12.5%	10%	15%	15%	5%	12.5%	25%	5%	100.0%	35%
UAT	12.5%	15%	15%	15%	5%	17.5%	15%	5%	100.0%	35%
Deploy/Close	15%	15%	15%	15%	5%	15%	5%	15%	100.0%	35%
	PM	CA	LD	AD	ID	QA MGR	TESTER	SA	Blended	
Rates	$ 110	$ 110	$ 110	$ 90	$ 75	$ 100	$ 70	$ 85	$ 94	

Figure 10: Sample of Summary Project Cost Report from Estimating Tool



		Total						QA	QA		
	ID	Hours	PM	CA	LD	AD	ID	MGR	TEST	SA	Cost
DEVELOPMENT											
Project Name											
Authentication	1	672	76	94	114	149	50	87	62	40	$ 64,840
Searching	2	562	64	79	95	124	41	73	52	33	$ 54,202
Tracking	3	882	100	124	149	195	65	114	82	53	$ 85,103
Contact Tracing	4	94	9	12	16	23	7	11	9	6	$ 8,962
Group Management	5	133	15	19	23	30	10	17	12	8	$ 12,836
Alerting	6	252	29	35	43	56	19	33	23	15	$ 24,315
Monitoring	7	478	54	67	81	106	35	62	44	28	$ 46,097
Hardware	8	0	0	0	0	0	0	0	0	0	$ -
Mobile Application	9	175	17	26	31	46	15	22	8	11	$ 16,991
Reporting	10	0	0	0	0	0	0	0	0	0	$ -
Sharing	11	25	2	3	4	8	2	3	1	2	$ 2,395
Reporting	12	46	5	6	8	11	4	6	3	3	$ 4,403
	13	0	0	0	0	0	0	0	0	0	$ -
Live Feed (Separate Budget)	14	0	0	0	0	0	0	0	0	0	$ -
Buisness Rules / Privacy	15	231	26	32	39	51	17	30	21	14	$ 22,289
0	16	0	0	0	0	0	0	0	0	0	$ -
	17	0	0	0	0	0	0	0	0	0	$ -
Web Site (Separate Budget)	18	0	0	0	0	0	0	0	0	0	$ -
Marketing Materials (Separate Budget)	19	0	0	0	0	0	0	0	0	0	$ -
Installation Code and Release Process	20	227	25	33	39	55	18	29	11	17	$ 22,070
Creative for Default Screens and Assets	21	210	24	30	36	47	16	27	20	13	$ 20,263
Manuals/Install instructions/etc	22	108	11	16	19	27	9	14	4	8	$ 10,510
Total		**4093**	**456**	**578**	**695**	**926**	**308**	**527**	**354**	**250**	**395275**

PRODUCT DEVELOPMENT TEAM AND PLATFORM

The development team structure for the proposed product should follow CMMI standard practices. A typical team includes:

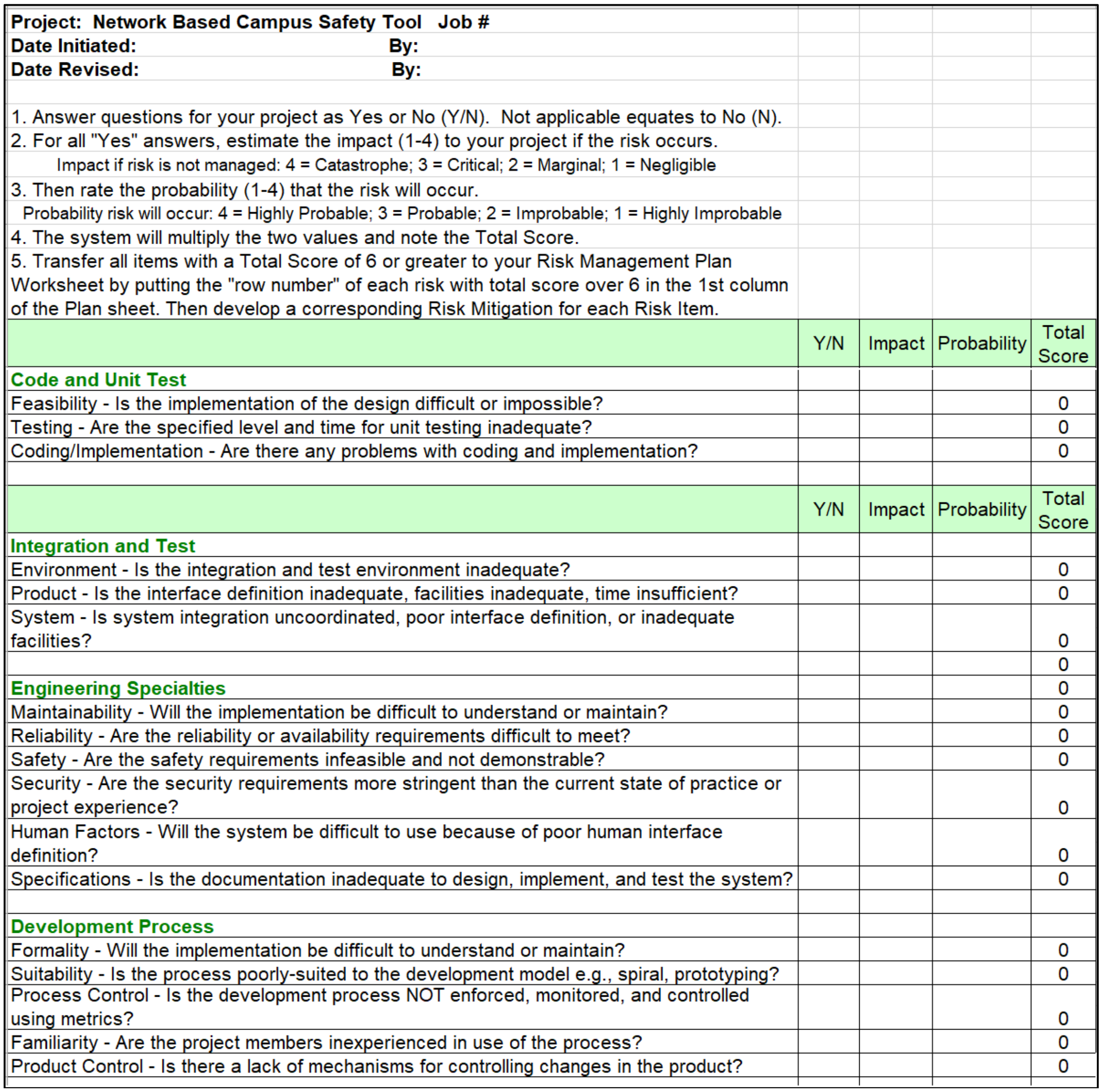
- PM – Project Manager
- CA – Chief Architect
- LD – Lead Developer
- AD – Associate Developer
- ID – Interface Developer
- QA MGR – Quality Assurance Manager
- TESTER – Software Tester
- SA – Systems Administrator, and others.

The CMMI Design Team (2010) discusses simulation, modeling, and prototyping as architectural considerations along with big data (e.g., wireless location service data for possible tens of thousands of devices), artificial intelligence and machine learning. The proposed product development platform, for example: LAMP (Linux, Apache, MySQL, Php), Ruby on Rails, .net, or another suitable web-based architecture is well integrated with current personal device/smartphone interfaces, while promoting maintainability, performance, self-documenting, as well as a supporting a layered architecture for upgradability and efficient interchange of a variety of wireless technology manufacturers. The CMMI decision analysis and resolution activity is a support process that contains specific practices addressing formal evaluation used during a CMMI technical solution design for selecting a superior technical solution from alternative solutions (CMMI Design Team, 2010). This process is ideal for evaluation of results from the IRB-approved Law Enforcement and Development Organization Survey, evaluation of use case suitability as a basis for proposed product design, and selection of technical components related to product performance.

QUALITY SOFTWARE-DEVELOPMENT-VENDOR SELECTION PROCESSES

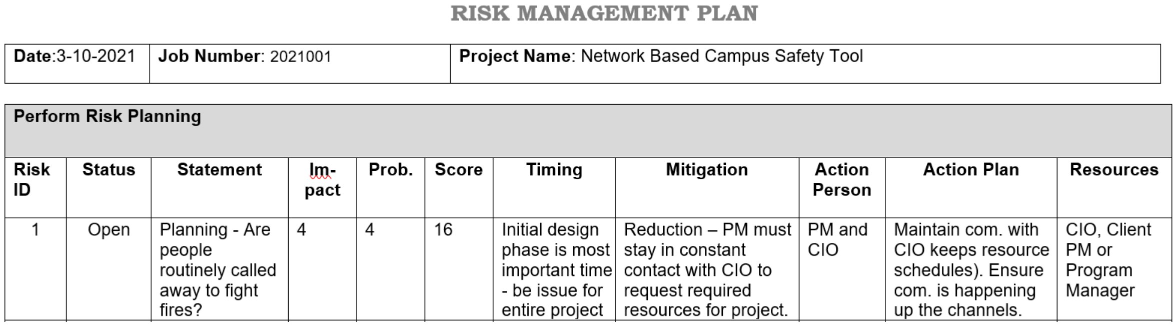
A CMMI SDLC calls for a risk management driven by a questionnaire (Figure 11). Any questionnaire high-risk items (i.e., total score of 6 or above) will have a specific risk management plan as shown in Figure 12. The risk management plan for each questionnaire high-risk item adds planning information including: status (open/closed), project timing or phase risk is most likely, mitigation method of one of several types including: 1) avoidance, 2) reduction, 3) transfer, and 4) protection: action person/role responsible for an action plan item, a specific action plan which are specific task(s) necessary for successful mitigation, and finally, resources which are specific individual(s), team(s), vendor(s), and/or facilities, etc. involved as part of an individual risk management plan item (Burwick, 2008; CMMI Development Team, 2010).

Figure 11: Sample Snippet of Risk Management Questionnaire



Project: Network Based Campus Safety Tool Job #				
Date Initiated: By:				
Date Revised: By:				
1. Answer questions for your project as Yes or No (Y/N). Not applicable equates to No (N).				
2. For all "Yes" answers, estimate the impact (1-4) to your project if the risk occurs.				
Impact if risk is not managed: 4 = Catastrophe; 3 = Critical; 2 = Marginal; 1 = Negligible				
3. Then rate the probability (1-4) that the risk will occur.				
Probability risk will occur: 4 = Highly Probable; 3 = Probable; 2 = Improbable; 1 = Highly Improbable				
4. The system will multiply the two values and note the Total Score.				
5. Transfer all items with a Total Score of 6 or greater to your Risk Management Plan Worksheet by putting the "row number" of each risk with total score over 6 in the 1st column of the Plan sheet. Then develop a corresponding Risk Mitigation for each Risk Item.				
	Y/N	Impact	Probability	Total Score
Code and Unit Test				
Feasibility - Is the implementation of the design difficult or impossible?				0
Testing - Are the specified level and time for unit testing inadequate?				0
Coding/Implementation - Are there any problems with coding and implementation?				0
	Y/N	Impact	Probability	Total Score
Integration and Test				
Environment - Is the integration and test environment inadequate?				0
Product - Is the interface definition inadequate, facilities inadequate, time insufficient?				0
System - Is system integration uncoordinated, poor interface definition, or inadequate facilities?				0
				0
Engineering Specialties				0
Maintainability - Will the implementation be difficult to understand or maintain?				0
Reliability - Are the reliability or availability requirements difficult to meet?				0
Safety - Are the safety requirements infeasible and not demonstrable?				0
Security - Are the security requirements more stringent than the current state of practice or project experience?				0
Human Factors - Will the system be difficult to use because of poor human interface definition?				0
Specifications - Is the documentation inadequate to design, implement, and test the system?				0
Development Process				
Formality - Will the implementation be difficult to understand or maintain?				0
Suitability - Is the process poorly-suited to the development model e.g., spiral, prototyping?				0
Process Control - Is the development process NOT enforced, monitored, and controlled using metrics?				0
Familiarity - Are the project members inexperienced in use of the process?				0
Product Control - Is there a lack of mechanisms for controlling changes in the product?				0

Figure 12: Sample Snippet of a Single Item within a Risk Management Plan



RISK MANAGEMENT PLAN

Date:3-10-2021	**Job Number**: 2021001	**Project Name**: Network Based Campus Safety Tool

Perform Risk Planning

Risk ID	Status	Statement	Impact	Prob.	Score	Timing	Mitigation	Action Person	Action Plan	Resources
1	Open	Planning - Are people routinely called away to fight fires?	4	4	16	Initial design phase is most important time - be issue for entire project	Reduction – PM must stay in constant contact with CIO to request required resources for project.	PM and CIO	Maintain com. with CIO keeps resource schedules). Ensure com. is happening up the channels.	CIO, Client PM or Program Manager

Finally, other important processes are used for selection of a quality software-development-vendor by vetting them through an RFP process (see Chapter 3 section regarding vendor response to a requirements and validation plan).

CONCLUSION

Software product design follows a formalized standard framework using various processes from CMMI. Actual project execution will likely layer additional process methods, for example, *agile* SDLC, a software development framework, like LAMP, or others. The final selection of these tools will be largely dependent and likely one familiar and preferred by whichever software development vendor/partner is awarded the project. The client sponsoring this software development project, through requiring the CMMI framework, will benefit from these and other formalized CMMI processes like decision analysis and response for particularly complex or costly decision-making situations (Burwick, 2008; CMMI Design Team, 2010) as well as supplier agreement management, of which the R&V Plan is a central part (Burwick, 2008; CMMI Design Team, 2010).

This chapter outlined processes which greatly enhance expected outcomes for developing a proposed enterprise college campus safety product and have it fully readied for higher education institution deployment.

CHAPTER FIVE: EVALUATION AND IMPLEMENTATION

INTRODUCTION

This chapter discusses how product design methods will be evaluated and system level deployment recommendations are given.

PRODUCT DESIGN EVALUATION

The IRB approved Law Enforcement and Development Organization Survey or specifically as executed, a law enforcement professional interview is used to support and verify product dissertation design information. The interview sought supplemental information and interview follow up regarding information gathered during prior use-case discovery work and sought to gather information regarding law enforcement incident response practices, investigative policy, and right-to-privacy implications, which informed development of new campus safety technology. The new software tool hopes to aid campus police during incident response and investigations for a variety of use scenarios, from incident response initiation to active incident investigation and resolution including:

1. Fill some gaps associated with incident response initiation understanding.
2. Confirm product use scenarios for realism, value added, and identification of any gaps associated with product features.
3. Discuss public's right-to-privacy vs. efficacy of officers keeping the public safe and apprehending offenders.

PRODUCT DEPLOYMENT

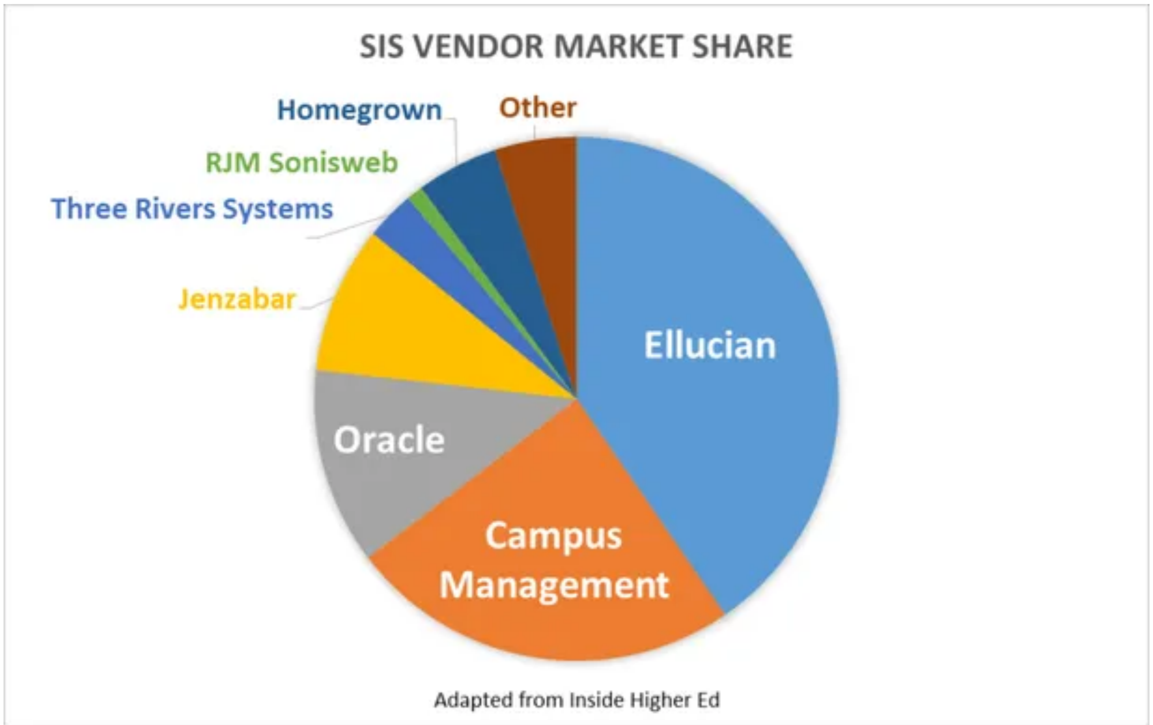
I spent over 25 years leading software development organizations for a variety of industries including computer-aided design, computer-aided engineering, scientific analysis and simulation, and internet-based process automation software for automotive OEMs and tier one automotive suppliers, among others. Associated with these roles, software development and deployment were carried out on a wide variety of software development and delivery platforms. Describing advantages and disadvantages as well as optimal choices of frameworks for a given software application type are tangential to this research and will not be provided. However, my experience indicates an internet-based software environment best suits this campus safety application and proposed use environment.

Software Development Environment and Programming Language

Various software languages and development frameworks are appropriate, starting with open-source systems such as LAMP to mainstay commercial systems such as Java and associated tools. These frameworks allow a level of scalability necessary to accommodate colleges of any size. Either is recommended as an abundance of development resources are readily available.

The latest container technology (makes interchanging similar software functions efficient and maintainable) is recommended to allow use of interchangeable components for a variety of wireless network technology and student information system manufacturers to be supported using manufacturer-specific API libraries interchangeably as product acceptance and industry penetration increases. Ellucian’s suite of higher education student information systems are highly recommended as the first campus SIS system to be supported because these products represent the largest market share of systems deployed for the higher education market as a somewhat dated Figure 13 shows.

Figure 13: Student Information System Market Share



Source: Straumsheim (2013)

Software Product Deployment Hardware

Given today’s circumstances, a specific hardware platform recommendation is less important than recommending software be developed within a virtual environment. Either of VMware or Dell Technologies’ Hyper-V hypervisor environments are leading choices. A virtual environment provides highly flexible deployment with advanced cybersecurity features on a wide variety of hardware platforms as well as providing great scalability allowing system deployment into a wide range of college sizes. This is key, as virtual computing environments can easily create provisions for colleges of a few thousand devices/students to large colleges having more than 100,000 devices, accommodated by adding more hardware. A sample hardware configuration for a typical environment is shown below for a campus of approximately 10,000 to 20,000 students. The actual number of servers needed would depend on a client deployment analysis to accommodate environment scale and assuming appropriate system redundancy.

- Two U rack mountable server with minimum of 20 storage drive bays.
- 768GB memory per HCI (hyper converged infrastructure) server
- Redundant power supplies
- Mirrored 32GB minimum SD cards
- Enterprise server manager
- 6 – 10Gb SFP+ network ports
- Out of band copper management port
- Total storage __.0TB all 12Gbps SAS SSD raw capacity/HCI server (4TB or less each)
- Cache drive configuration requires adequate size for capacity of write intensive SSD.
- Over 40,000 IOPS per HCI server
- 264 vCPU per side
- 4.6TB memory per side
- 342.0TB raw capacity per side
- 3-5-year next business day hardware support
- 3-5 years of 24x7 technical support

Network switch recommendation (MFG independent) would typically include:

- 48 Port 10Gb SFP+
- Uplink 10/40GB QSFP
- Dual power supplies

- 32Mb or more packet buffer
- Four or more fans
- Including enterprise protocols associated with ToR (top of rack) switching
- 5-year next business day hardware support
- 5 years of 24x7 technical support

Best practices would dictate a development environment used for product development should, as closely as is practical, match this same deployment hardware architecture.

Training for Development Team and Product End Users

Selected product development partner training, if needed, for CMMI is documented and addressed by the CMMI Design Team (2010) and Burwick (2008). However, selection criteria for a development partner should require expertise with CMMI process, negating CMMI training per se; however, documentation also discusses end-user training. Further training direction is discussed by Alistair (2001).

Product Marketing

Obviously, higher education is a primary sales target, starting with those whose SIS system represents the largest market share of higher education colleges; namely Ellucian. Simultaneously, target colleges whose wireless networks use controllerless wireless network technology with an open API interface making integration with student and employee information easily feasible, for example Extreme Networks (formally Aerohive Networks).

Target community college administrators, including presidents and administrators responsible for campus safety and more specifically campus police departments and campus security, as well as information technology administrators. These administrators have direct decision-making authority and subject-matter awareness regarding the importance of improved campus safety methods and the technical plausibility of deploying a system such as presented as part of this product research.

Product Sales

Many models exist for sales of such a software product. Pricing models range from a flat fee plus maintenance and support to models as highly granular as price per student or device monitorable; which can be difficult to determine due to fluctuating numbers of students throughout an academic year between full-time vs part-time vs continuing education students. Higher education environments often have software pricing based on an equivalent full-time student calculation; this would be appropriate for our current situation. Additionally, support and maintenance are typically set at approximately 15% to 20% of the subscription or initial purchase price. Enterprise software licenses are typically annual subscriptions or an enterprise contract of one, three, or five years, providing clients with annual price increase protection.

Sales channels for our new campus safety enterprise software product would follow a product life cycle model using a new technology adoption curve, such as the one described in *Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers* (Moore, 1991), which defines a typical client culture for initial potential target colleges. Such initial potential customers would be characterized as early adopters according to Moore and PeopleWiz Consulting, (2013). This product can represent a transformational change for campus safety for colleges (Smyre & Richardson, 2016), preparing us for a world that doesn’t exist yet. Selling to early adopters is most likely done by product concept developers first, then by sales reps or value-added resellers, and when product market penetration is mature, a software manufacturer direct sales force is most typical and profitable.

ONGOING PRODUCT SUPPORT AND MAINTENANCE

A typical operations and support specification would include the items listed in Table 2.

Table 2: Typical Operations and Support Requirements for Enterprise Software

REQUIREMENT	REQUIREMENTS CRITERIA
Implementation Support	Provides complete turnkey on-site implementation and project management support.
Customer Support	Provides toll free customer support 24 hrs./day, 7 days/week.
Production Environment	Production environment monitoring and support for 3 months.
Training	Provides onsite training to technicians and end users.
Software Updates	Provides future software releases and updates to all applications as part of regular software maintenance fees.
Technical Documentation	Provides technical documentation for support staff, including system overviews, design, flowcharts, and file layouts.
User Manuals	Provide complete set of user manuals for software applications documenting and explaining system features and functions.

CONCLUSION

In this chapter, I described proposed product design evaluation methods and makes recommendations on a development environment, deployment software and hardware, training strategies, product marketing targets and rational, and sales methods and tactics. These methods are based on enterprise software industry standard and best practices, as well as my over 30 years of experience regarding software development and all facets of related fields necessary for successful execution of such a product commercialization.

This chapter provided a framework and roadmap for a full software product life cycle, from concept to deployment to long term product support and maintenance. Following this roadmap provides this endeavor a high likelihood of success.

CHAPTER SIX: CONCLUSION AND IMPLICATIONS

INTRODUCTION

Need for improved personal safety and security change throughout our world is accelerating at a rate few could imagine. We have seen increasing senseless campus shootings, rioting within our nation's capital, escalating race-related hate crime, and a worldwide pandemic requiring trillions of stimulus dollars to keep our economy afloat. Safety has taken on new dimensions leading to global life changes we barely anticipated just one year ago. Using technology to keep ourselves safe is no longer an option. How we do it effectively and ethically is our most important question. Thoughtful safeguards for scope and focus of incident investigations to balance actionable intelligence with privacy protections are paramount.

This product dissertation describes a new product for technology improved campus safety through the creation of a wireless network-based campus police incident response tool focused on person-of-interest and witness identification, potential victim protection, and contact tracing and driving transformational change for campus and student safety. The technology exists and can realistically fulfill expectations. The challenge is stakeholder acceptance and bringing together stakeholders and technology companies via a cooperative effort to embrace change and make any cultural and legislative early-adopter accommodations required during early deployments of this new system.

IMPLICATIONS FOR FURTHER STUDY AND DEVELOPMENT

This dissertation discusses an initial version of a technical improvement to incident response and campus safety. However, further improvements through seamless integration between on campus security systems can take these improvements even further. Surveillance camera systems currently apply a universal time code tagging on video footage. These time codes can be synchronized with proposed product time coding for even more concurrent real-time situational visibility of incidents of interest during and after they occur. Such seamless integration would continue to improve law enforcement operational efficiency and success.

Likewise, as fusion center concepts mature and become increasingly common, integration of our proposed product gives a fuller picture of situations and subjects when information is most needed, in near-real-time or as soon after an incident as possible during the magic 48 hours so critical to successful incident resolution and apprehension of perpetrators. Fusion centers are designed to share information similar to systems designed to comply with HIPAA (Health Information Portability and Accountability Act) with common data formatting, data structures, and communication protocols. Fusion centers attempt to provide similar protected access to an array of information for law enforcement like criminal records, DMV records, mental health records, previous non-criminal incident reports, known associates, behavior patterns, and more. Information sharing, by its very nature, shortens and unburdens laborious investigative processes.

Person-of-interest alerting can be added as a pre-emptive capability to alert proper officials (law enforcement, HR, administration) when a given individual comes on campus or, like contact tracing, comes within a specified distance to a person having an active personal protective order. This type of capability requires taking privacy preserving surveillance to another level and may still be too controversial for our first version.

Finally, Land (2015) discuses participatory fact-finding where citizenry (i.e., students) participate with law enforcement on incident response and investigation via various modes and technologies. Development of these new technologies for human rights investigations through new technologies can advance future human rights fact-finding. This product identifies potential witnesses within proximity to an active or prior incident of interest who all have electronic devices capable of providing real-time situational data and potentially recording such. Automatically identifying these individuals and these devices provides a plethora of potential methods to capture information like remotely turning on smart phone microphones and/or cameras. The challenge is to do so ethically while applying privacy preserving surveillance practices.

IMPLICATIONS TO PRIVACY AND STATE AND FEDERAL COMPLIANCE

Chapter one and two discussed keeping students safe and how their right to privacy can be at odds when applying such a technical solution to campus safety and incident response. Product safeguards will exist preventing device association with an individual unless minimum rationale exists for investigation, protecting data, and privacy. Additionally, advances regarding privacy-preserving surveillance methods have started a conversation and development of processes with a goal of assuring both safety and privacy protection can coexist. A future enhancement to our product might be to integrate a software safety method such as a questionnaire asking, “Is this an emergency situation?” before a software is utilized as well as providing a warning against nonemergency use. I imagine questions similar to those posed on an application for a law enforcement search warrant or subpoena. Further study is needed to formalize and expand methods for enhanced auditability and oversight leading to use of this technology via a properly narrow scope of applicability. The goal being to provide an environment of campus safety and improved incident response acceptable to all stakeholders.

Protection of private data or PII has become paramount while facing escalating cybercrime. In recent years, cybercrime has become dramatically more sophisticated with funding levels at a nation-state level. Technological protection, such as encryption of data at rest and in-flight, and data anonymization for privacy-preserving surveillance should be provided by prescribed separation between wireless network MAC address device identification and student information system student or user PII until probable cause is adequately established. Friedewald et al. (2010), Wong et al. (2020), and Hamam and Derhab (2021) discuss standard data protection frameworks and the OWASP top ten most common data protection problems, proper policy creation, and countermeasures guaranteeing protection against most severe attacks and preventing several unknown exploits. Turner (2017) describes a portfolio of common enterprise information security technology tools available to protect data and privacy which continues to evolve, hopefully at a faster pace compared to cybercrime technological advancement. Such technologies should be brought to bear in parallel with deployment of such incident response technology improvements.

A Word of Warning

One size does not fit all when it comes to security. Perception differences regarding protection and actual deterrence offered by security tactics vary by academic year and student age, making each college campus unique. Actions taken after a violent event focusing on traditional technical solutions (increased use of technology and enforcement; cameras, access-control, and armed guardians) may not provide desired benefit of long-term cultural change and less violence. Individual school characteristics are consistent general public indicators of prevalent crimes to prevent. Rather than ramping up technical security measures, a better starting point may be to focus on larger societal-level problems leading to overly negative levels of school characteristics. “Attempting to reduce conflict, create mediation programs, and establish anti-bullying strategies both on and off campus may all prove beneficial and could be a more effective use of school and law enforcement resources” (Crawford & Burns, 2015, p. 644-645). A trend toward tolerance and cultural co-existence has equal chance to reduce campus crime.

CONCLUSION

This research has attempted to anticipate most big challenges to be overcome through deployment of a new campus safety software solution with suggested direction for remediation. Like all new approaches to keep our citizenry and, more specifically, our students safe through making law enforcement more effective, comes with a need for increased education, cooperation, vigilance regarding privacy, and compromise from all sides.

The initial system features represent only a small portion of what can be provided. Further qualitative and quantitative system evaluation can lead to future enhancements and system integrations to optimize and improve solutions recommended here. Therefore, sometime after this technology is deployed, further qualitative and/or quantitative studies can be performed regarding efficacy of incident prevention, removal of potential victims from harm’s way during an active dangerous incident, and/or historic or active contact tracing needed so prevalently today for managing COVID-19 spread (Dionicio, 2020; Wallace, 2020). Additionally, future research can expand parameters regarding administrative hurdles to improve general applicability.

REFERENCES

Ackie, M., Gibson, D., Hoffman, E., Marion, N., & Guobadia-Serioux, I. (2020). *Final title IX regulations adopt sweeping changes for handling sexual harassment claims at institutions of higher education*. Littler. https://www.littler.com/publication-press/publication/final-title-ix-regulations-adopt-sweeping-changes-handling-sexual

Alistair, C. (2001). *Writing effective use cases.* Pearson.

Anderson. G. (2020, June 10). Community colleges burdened by new Title IX regulations. *Inside Higher Ed*. https://insidehighered.com/print/news/2020/06/10/community-colleges-burdened-new-title-ix-regulations

Bai, C., & Shen, H. (2015). *Radio frequency identification technology-based campus student safety management system*. European Patent Office*.*

Baniukevic, A., Sabonis, D., Jensen, C., & Hua, L. (2011). Improving Wi-Fi-based indoor positioning using bluetooth add-ons. In *IEEE 12th International Conference on Mobile Data Management, 1*, 246-255. https://doi.org/10.1109/ MDM.2011.50

Banjo, P. (2012). *Use of mobile phones in natural disasters: A case study of the Haiti 2010 earthquake* [Unpublished doctoral dissertation]. Bucks New University.

Becker, R. (2005). *Criminal investigation* (2nd ed.) Jones and Bartlett.

Blackwell, T. (2019). *The top five technology trends for campus safety in 2019*. International Association of Campus Law Enforcement Administrators. https://www.iaclea.org/member-news/2019/03/04/top-five-tech-trends-for-campus-safety-in-2019/

Bolla, E. (2019). The assault on campus assault: The conflicts between local law enforcement, FERPA, and Title IX. *Boston College Law Review, 60*(5), 1379-1414. https://lawdigitalcommons.bc.edu/bclr/vol60/iss5/4

Broeders, D., Schrijvers, E., van der Sloot, B., van Brakel, R., de Hoog, J., & Hirsch Ballin, E. (2017) Big data and security policies: Towards a framework for regulating the phases of analytics and use of big data. *Computer Law and Security Review, Vol. 33* (3): 309-323. https://doi.org/10.1016/j.clsr.2017.03.002

Burwick, D. M. (2008). *How to implement the CMMI: Real process improvement using proven solutions.* Business and Personal Solutions Publishing.

Butler, A., & Lafreniere, K. (2010). Campus reactions to mass notification. *Journal of College Student Development, 51*(4), 436-439. https://doi.org/10.1353/csd.0.0145

Casella, R. (2003). The false allure of security technologies. *Social Justice, 30*(3), 82-93. https://www.jstor.org/stable/29768210

Chang, S. (2001). *Handbook of software engineering and knowledge engineering* (Vol. 1). World Scientific.

CMMI Product Team. (2010). *CMMI for development, Version 1.3 (CMU/SEI-2010-TR-033)*. Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu. edu/library/asset-view.cfm?AssetID=9661

Cornell University Law School. (2021, August 15) *Probable cause*. https://www.law.cornell.edu/ wex/probable_cause

Crawford, C., & Burns, R. (2015). Preventing school violence: Assessing armed guardians, school policy, and context. *Policing*, 38(4), 631-647. https://doi.org/10.1108/PIJPSM-01-2015-0002

Dionicio, R. (2020) *Contact tracing over Wi-Fi*. Packet6. https://packet6.com/contact-tracing-wifi/

Electronic Privacy Information Center. (2020, Nov. 27). Surveillance oversight: *PATRIOT Act.* https://epic.org/issues/ surveillance-oversight/patriot-act/

Feigenbaum, J. (2019). Encryption and surveillance. *Communications of the ACM, 62*(5), 27-29. https://doi.org/10.1145/3319079

Figueiras, J., & Frattasi, S. (2010). *Mobile positioning and tracking: From conventional to cooperative techniques*. Wiley.

FindLaw. (2019). *Is there a "right to privacy" amendment?* https://www.findlaw.com/ injury/torts-and-personal-injuries/is-there-a-right-to-privacy-amendment.html

Fletcher, P. C., & Bryden, P. J. (2007). Preliminary examination of safety issues on a university campus: Personal safety practices, beliefs, and attitudes of female faculty and staff. *College Student Journal, 41*(4), 1149-1162.

Friedewald, M., Wright, D., Gutwirth, S., & Mordini, E. (2010). Privacy, data protection, and emerging sciences and technologies: Towards a common framework. *Innovation: The European Journal of Social Science Research*, *23*(1), 61-67. https://doi.org/10.1080/ 13511611003791182

Galitz, W. O. (2007*). The essential guide to user interface design: An introduction to GUI design principles and techniques* (3rd ed.). Wiley.

Gilmore, H. (2016). Developing a comprehensive campus security program: A case of Schoolcraft College [Unpublished doctoral dissertation]. *Ferris State University*.

Goodman, R. (2009). Keeping our campuses and communities safe. *Journal of Strategic Security*, *2*(3), 65-70. https://doi.org/10.5038/1944-0472.2.3.6

Gow, G., Mcgee, T., Townsend, D., Anderson, P., & Varnhagen, S. (2009). Communication technology, emergency alerts, and campus safety. *IEEE Technology and Society Magazine, 28*(2), 34-41. https://doi.org/10.1109/MTS.2009.932797

Green, M. (1999). *The appropriate and effective use of security technologies in U. S. schools*. National Institute of Justice Research report (NCJ 178265). https://www.ncjrs.gov/school/178265.pdf

Griffin, O. R. (2016). View of campus safety law in higher education and the merits of enterprise risk management. *Wayne Law Review*, 61(2), 379-406.

Gursoy, M. E., Inan, A., Nergiz, M. E., & Saygin, Y. (2016). Privacy-preserving learning analytics: challenges and techniques. *IEEE Transactions on Learning technologies, 10*(1), 68-81. https://doi.org/10.1109/TLT.2016.2607747

Hamam, H., & Derhab, A. (2021). An OWASP top ten driven survey on web application protection methods. In J. Garcia-Alfaro, J. Leneutre, N. Cuppens, & R. Yaich (Eds.), *Risks and security of internet and systems. CRiSIS 2020. Lecture Notes in Computer Science, vol 12528.* Springer. https://doi.org/10.1007/978-3-030-68887-5_14

Heidt, D. M. & Turner, P. R. (2020). *Campus overwatch: Use cases and real-life scenarios. Deductive Data* [Unpublished manuscript].

Hites, L., Fifolt, M., Beck, H., Su, W., Kerbawy, S., Wakelee, J., & Nassel, A. (2013). A geospatial mixed methods approach to assessing campus safety. *Evaluation Review, 37*(5), 347-369. https://doi.org/10.1177/0193841X13509815

Ilkhechi, A., Korpeoglu, I., Güdükbay, U., & Ulusoy, Ö. (2017). PETAL: A fully distributed location service for wireless ad hoc networks. *Journal of Network and Computer Applications, 83*, 1-11. https://doi.org/10.1016/j.jnca.2017.01.021

Independence Hall Association. (2020). *Bill of Rights and later amendments*. ushistory.org/documents/amendments.htm

Intersoft Consulting. (2020*). Information to be provided where personal data are collected from the data subject* (Art 13 GDPR). https://gdpr-info.eu/art-13-gdpr/

Jennings, W. G., Khey, D. N., Maskaly, J. & Donner, C. M. (2011). Evaluating the relationship between law enforcement and school security measures and violent crime in schools. *Journal of Police Crisis Negotiations, 11*(2), 109-124.

Kim, K., & Kim, M. (2012). RFID-based location-sensing system for safety management. *Personal and Ubiquitous Computing, 16*(3), 235-243. https://doi.org/10.1007/s00779-011-0394-0

Kumar, M., & Rashid, E. (2018). An efficient software development life cycle model for developing software project. *International Journal of Education and Management Engineering, 8*(6), 59-68. https://doi.org/10.5815/ijeme.2018.06.06

Kyle, M. J., Schafer, J. A., Burruss, G. W., & Giblin, M. J. (2017). Perceptions of campus safety policies: Contrasting the views of students with faculty and staff. *American Journal of Criminal Justice*, *42*(3), 644-667. https://doi.org/10.1007/s12103-016-9379-x

Lake, P. (2013, July 15). What the new campus-safety center can accomplish. *Chronicle of Higher Education, 59*(42). https://www.chronicle.com/article/What-the-New-Campus-Safety/140321

Lambert, D. (2010). Intelligence-led policing in a fusion center. *The FBI Law Enforcement Bulletin*, *79*(12), 1-6.

Land, M. K. (2015). Democratizing human rights fact-finding. In P. Alston & S. Knuckey (Eds.), *The transformation of human rights fact-finding* (pp. 399-424). Oxford University Press.

Land, M., & Meier, P. (2012). *#ICT4HR: Information and communication technologies for human rights.* World Bank Publications.

Madison, J., Hamilton, A., Jay, J. (1787). *The Constitution of the United States.* https://constitutioncenter.org/media/files/constitution.pdf

Maguire, D. (2008). *ArcGIS: General purpose GIS software system*. Springer Science+Business Media.

Mahanti, R., Neogi, M. S., & Bhattacherjee, V. (2012). Factors affecting the choice of software life cycle models in the software industry - An empirical study. *Journal of Computer Science 8*(8), 1253-1262. https://doi.org/10.3844/jcssp.2012.1253.1262

Malaney, R. A. (2014). *Location-enabled security services in wireless network*. European Patent Office.

Marques, N., Meneses, F., & Moreira, A. (2012, November*). Combining similarity functions and majority rules for multi-building, multi-floor, WiFi positioning*. 2012 International Conference on Indoor Positioning and Indoor Navigation (pp. 1-9). https://doi.org/10. 1109/IPIN.2012.6418937

McPherson, E. (2015). Digital human rights reporting by civilian witnesses: Surmounting the verification barrier. In R. A. Lind (Ed.), *Producing theory 2.0: The intersection of audiences and production in a digital world* (pp. 193-209). Peter Lang.

Mendoza, S. (2014). Student safety, security and response time: Is your campus in compliance? *Hispanic Outlook in Higher Education Magazine, 24*(23), 13.

Michigan Judiciary. (2021). *Instructions for preparing affidavit and search warrant.* https://courts.michigan.gov/Administration/SCAO/Forms/courtforms/mc231.pdf

Mitchell, A., & Swobodzinski, K. (2013). Building a crime analyst: One training module at a time. *The Police Chief*, *80*(11), 34.

Moore, G. A. (1991). *Crossing the chasm: Marketing and selling technology products to mainstream customers*. Harper Business.

National Center for Campus Public Safety. (2016*). Institutionalizing the Clery Act at institutions of higher education: Findings of a focus group of college and university compliance executives*. https://www.nccpsafety.org/assets/files/library/Institutionalizing_Clery_ Report_ FINAL.pdf.

National Incident Management System. (2010a) *NIMS implementation activities for schools and institutions of higher education.* https://rems.ed.gov/docs/NIMS_ ComprehensiveGuidanceActivities_2009-2010.pdf

National Incident Management System. (2010b) *Checklist: NIMS implementation activities for schools and institutions of higher education*. https://rems.ed.gov/docs/NIMS_ ImplementationActivitiesChecklist_2009-2010.pdf

National Incident Management System. (2010c) *FY 2010 NIMS training for K-12 schools and institutions of higher education*. https://rems.ed.gov/docs/NIMS_ KeyPersonnelTraining_2009-2010.pdf

National Incident Management System. (2010d) *Frequently asked questions about NIMS implementation activities for schools and institutions of higher education*. https://rems.ed.gov/docs/NIMS_FAQ_2009-2010.pdf

National Incident Management System. (2018). *Cybersecurity considerations for institutions of higher education. Cybersecurity for Higher Ed Fact Sheet*. https://rems.ed.gov/docs/ Cybersecurity_Considerations_for_Higher_ed_Fact_Sheet_508C.pdf

Ndzukula, S., Ramotsoela, T., Silva, B., & Hancke, G. (2017). *A bluetooth low energy-based system for personnel tracking*. 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017, 8435-8440. https://doi.org/10.1109/ IECON.2017.8217481

Nobles, M., Fox, K., Khey, D., & Lizotte, A. (2013). Community and campus crime: A geospatial examination of the clery act. *Crime and Delinquency, 59*(8), 1131-1156. https://doi.org/ 10.1177/0011128710372188

Oxedine, C. E., (2013). *Analysis of volunteered geographic information for improved situational awareness during no-notice emergencies* [Unpublished doctoral Dissertation]. George Mason University.

Padania, S., Gregory, S., Alberdingk-Thijm, Y., & Nunez, B. (2011). *Cameras everywhere: Current challenges and opportunities at the intersection of human rights, video and technology.* Witness.

Page, S., Freberg, K., & Saling, K. (2013). Emerging media crisis value model: A comparison of relevant, timely message strategies for emergency events. *Journal of Strategic Security*, 6(2), 20-31. https://doi.org/10.5038/1944-0472.6.2.2

PeopleWiz Consulting. (2013, Jan 13). *A comparison of 5 popular models for managing business change* [PowerPoint slides]. http://www.slideshare.net/peoplewizconsulting/change-management-models-a-comparison

Reitzig, R. W., Goldenson, D. R., Gibson, D., & Cavanaugh, M. R. (2007, March 26-29). *Calculating CMMI-based ROI why, when, what, and how?* 19th Annual SEPG Conference, Austin, TX, USA. https://resources.sei.cmu.edu/asset_files/Presentation/2006_017_001_23991.pdf

Saeed, A., Usmani, R. S. A., Akram, H., Saqlain, S. M., & Ghani, A. (2017). The impact of capability maturity model integration on return on investment in IT industry: An expository case study. *Engineering, Technology, and Applied Science Research 7*(6), 2189-2193. https://doi.org/10.48084/etasr.1291

Schafer, J., Heiple, E., Giblin, M., & Burruss, G. (2010). Critical incident preparedness and response on post-secondary campuses. *Journal of Criminal Justice, 38*(3), 311-317. https://doi.org/10.1016/j.jcrimjus.2010.03.005

Schoolcraft College. (2019). 2019 Schoolcraft College annual security report. https://www.schoolcraft.edu/docs/librariesprovider28/Annual-Security-Reports/2019asr_updated1111219.pdf?sfvrsn=8160d8b5_4

Schumaker, D., & Karpovich, J. (2018). In-car video proves valuable in university security operations. *Security*, *55*(7), 26-27.

Segal, A., Ford, B., & Feigenbaum, J. (2014, August 18). *Catching bandits and only bandits: Privacy-preserving intersection warrants for lawful surveillance.* 4th USENIX Workshop on Free and Open Communications on the Internet. San Diego, CA, United States. https://www.usenix.org/system/files/conference/foci14/foci14-segal.pdf

Seo, D., Torabi, M. R., Sa, J., & Blair, E. H. (2012). Campus violence preparedness of U. S. college campuses. *Security Journal*, 25(3), 199-211. https://doi.org/10.1057/sj.2011.18

Smyre, R., & Richardson, N. (2016). *Preparing for a world that doesn't exist – yet: Framing a second enlightenment to create communities of the future*. John Hunt.

Snowden, E. (2019). *Permanent record.* Macmillan.

Stader, D., & Williams-Cunningham, J. (2017). Campus sexual assault, institutional betrayal, and Title IX. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, *90*(5-6), 198-202. https://doi.org/10.1080/00098655.2017.1361287

State of California Department of Justice. (2020). *California consumer privacy act (CCPA).* https://www.oag.ca.gov/privacy/ccpa

Stowell, H. G. (2018). A safety strategy on campus. *Security Management*, *62*(6), 44. https://www.asisonline.org/security-management-magazine/articles/2018/06/a-safety-strategy-on-campus/

Straumsheim, C. (2013). Workday enters SIS market. Inside Higher Ed. https://www.insidehighered.com/news/2013/09/11/workday-introduce-cloud-based-student-information-system-2014

Student Right-to-Know and Campus Security Act, Pub. L. 101-542, 104 Stat. 2381. (1990). https://www.govinfo.gov/content/pkg/STATUTE-104/pdf/STATUTE-104-Pg2381.pdf#page=1

Sweeney, L. (2005). Privacy-preserving surveillance using selective revelation. *IEEE Intelligent Systems, 1*, 83-84.

Taylor, L., Floridi, L., Van der Sloot, B. (Eds.). (2017) *Group privacy: New challenges of data technologies*. Springer.

Taylor, R., & Russell, A. (2012). The failure of police fusion centers and the concept of a national intelligence sharing plan. *Police Practice and Research*. *13*(2) 184-200. https://doi.org/10.1080/15614263.2011.581448

Thompson, R. M., & Cole, J. P. (2015). Stored communications act: Reform of the Electronic Communications Privacy Act (ECPA). https://fas.org/sgp/crs/misc/R44036.pdf

Turner, P. R. (2017, September 13-14). *The enterprise IT security portfolio: A technological survey* [PowerPoint slides; Conference session]. SecureWorld 2017, Detroit, MI, United States.

U. S. Department of Education. (2004, Sept 21). *Legislative history of major FERPA provisions*. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/ferpaleghistory.pdf

U. S. Department of Education. (2020, Sept 8). *Part 106 nondiscrimination of the basis of sex in education programs or activities receiving federal financial assistance.* https://www2.ed.gov/policy/rights/reg/ocr/edlite-34cfr106.html

U. S. Department of Education. (2020, Sept. 21). *Family Educational Rights and Privacy Act regulation*s. https://www.ecfr.gov/current/title-34/subtitle-A/part-99

U. S. Department of Education, Office of Post-Secondary Education. (2016). *The handbook for campus safety and security reporting.* http://www.ed.gov/admins/lead/ safety/campus.html

U. S. Department of Justice, Office of Community Oriented Policing Services. (2005). *National summit on campus public safety: Strategies for colleges and universities in a homeland security environment* (ED486269) ERIC. https://files.eric.ed.gov/fulltext/ED486269.pdf

Ulrich, K. T., Eppinger, S. D., Yang, M. C. (2020) *Product design and development* (7th ed.). McGraw Hill.

USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. (2001) https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

USA Patriot Improvement and Reauthorization Act of 2006, Pub. L. No. 109-177, 192 Stat. 120. (2006). https://www.congress.gov/109/plaws/publ177/PLAW-109publ177.htm

Vanderhyden, P. (2018). *Human-centered design* [Unpublished PowerPoint slides]. Design Center of Wayne County Community College District.

Vanjale, M. S., Deshpande, A., Pawale, K., & Bhagwat, P. (2014). Automatic security system based on wireless sensor network and GSM technology. *International Journal of Engineering Research and Technology 3*(4), 467-470. https://www.ijert.org/research/automatic-security-system-based-on-wireless-sensor-network-and-gsm-technology-IJERTV3IS040604.pdf

Vazquez-Llorente, R. & Wall, I. (Eds.). (2014). *Communications technology and humanitarian delivery: Challenges and opportunities for security risk management*. European Interagency Security Forum. https://reliefweb.int/sites/reliefweb.int/files/resources/EISF_Communications%20Technology%20and%20SRM_October%202014.pdf

Violence Against Women Reauthorization Act of 2013, Pub. L. No. 113-4, 127 Sat. 54. (2013). https://www.congress.gov/bill/113th-congress/senate-bill/47

Wallace, B. (2020). Ultra-wideband tech powers COVID-19 contact tracing tool for enterprises. *NETWORK Computing*. https://www.networkcomputing.com/wireless-infrastructure/ultra-wideband-tech-powers-covid-19-contact-tracing-tools-enterprises

Wang, W., & Xue, G. (2006). A cost-minimization algorithm for fast location tracking in mobile wireless networks. *Computer Networks*, *50*(15), 2713–2726. https://doi.org/10.1016/j.comnet.2005.09.035

Wardell III, C., & San Su, Y. (2011). *2011 Social media + Emergency management camp: Transforming the response enterprise.* Wilson Center. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/SMEM_Report.pdf

White, S. K. (2021). What is CMMI? A model for optimizing development processes. *CIO, IDG Communications*. https://www.cio.com/article/274530/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html

Winn, Z. (2018, March 13). Explaining Florida's new school safety law. *Campus Safety.* https://www.campussafetymagazine.com/safety/explaining-floridas-new-school-safety-law/

Wong, J., Henderson, T., & Ball, K. (2020, September 15-17). *Data protection for the common good: Developing a framework for a data protection-focused data commons*. https://doi.org/10.5281/zenodo.3965670

APPENDIX A: USE CASES AND REAL-LIFE SCENARIOS

Introduction

Campus overwatch: The use cases and real-life scenarios have been documented by Heidt and Turner (2020) and a full set can be provided upon request. Following is a short example of one documented use case for reference:

Identify people within proximity of an incident

At 0900 a window was broken on campus.

At 0915 law enforcement officers' surveys the scene.

At 0930 Law enforcement officers use proposed product to identify witnesses nearby at 0900.

At 0931 Law enforcement officers have a List of 10 people within 20 feet of broken window along with names, photo ID, phone numbers, and emails.

At 0932 Law enforcement officer calls first witness. Suzy describes a 6'2" Caucasian man with a beard throwing a football hitting window and shattered it.

At 0940 Law enforcement officer reviews picture IDs of those systems identifies closely located and sees a Caucasian man with a beard (Ben) is one of 10 people within 20 feet of incident at 0900

At 0942 Law enforcement officers Calls Ben and asks him if he knows anything about a broken window on campus.

At 0943 Ben admits he accidently broke window while playing football.

Note on Intellectual Property:

The fully documented set of Use Cases represent researcher intellectual property and will only be provided to those involved with product commercialization.

APPENDIX B: IRB APPROVAL LETTER

FERRIS STATE UNIVERSITY

INSTITUTIONAL REVIEW BOARD
1010 Campus Drive FLITE 410 Big Rapids, MI 49307
www.ferris.edu/irb

Date: April 20, 2021

To: Susan DeCamillis, EdD and Patrick Turner
From: Gregory Wellman, R.Ph, Ph.D, IRB Chair
Re: IRB Application *IRB-FY20-21-93 Technology Improved Campus Safety: Wireless Network-based Campus Police Incident Response, Person of Interest and Witness Identification, Potential Victim Protection, and Contact Tracing*

The Ferris State University Institutional Review Board (IRB) has reviewed your application for using human subjects in the study, *Technology Improved Campus Safety: Wireless Network-based Campus Police Incident Response, Person of Interest and Witness Identification, Potential Victim Protection, and Contact Tracing(IRB-FY20-21-93)* and approved this project under Federal Regulations Exempt Category 2.(ii). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording).
Any disclosure of the human subjects' responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation.

Your protocol has been assigned project number IRB-FY20-21-93. Approval mandates that you follow all University policy and procedures, in addition to applicable governmental regulations. Approval applies only to the activities described in the protocol submission; should revisions need to be made, all materials must be approved by the IRB prior to initiation. In addition, the IRB must be made aware of any serious and unexpected and/or unanticipated adverse events as well as complaints and non-compliance issues.

This project has been granted a waiver of consent documentation; signatures of participants need not be collected. Although not documented, informed consent is a process beginning with a description of the study and participant rights, with the assurance of participant understanding. Informed consent must be provided, even when documentation is waived, and continue throughout the study. As mandated by Title 45 Code of Federal Regulations, Part 46 (45 CFR 46) the IRB requires submission of annual status reports during the life of the research project and a Final Report Form upon study completion. Thank you for your compliance with these guidelines and best wishes for a successful research endeavor. Please let us know if the IRB can be of any future assistance.

Regards,

Gregory Wellman, R.Ph, Ph.D, IRB Chair
Ferris State University Institutional Review Board