



DEPARTMENT OF THE ARMY
OFFICE OF THE GENERAL COUNSEL
104 ARMY PENTAGON
WASHINGTON DC 20310-0104



REPLY TO THE ATTENTION OF:
SAGC A4-09-394c

June 17, 2009

MEMORANDUM FOR ARMY CHIEF INFORMATION OFFICER

SUBJECT: Use of Social Media in the Army

References

- a. DoDD 5230.09, Clearance of DoD Information for Public Release, 22 August 2008.
- b. DoDD 5410.18, Community Relations, Public Affairs Community Relations Policy, (certified current to 30 May 2007).
- c. DoDI 5410.19, Public Affairs Community Relations Policy Implementation.
- d. DOD 5500.7-R, Joint Ethics Regulation, 29 November 2007.
- e. Army regulation 25-1, Army Knowledge Management and Information Technology Management, 4 December 2008.
- f. Army Regulation 360- I, The Army Public Affairs program, 15 September 2000.
- g. US Central Command Regulation 360-5, Community Relations, 7 February 2007.
- h. Memorandum from Deputy Secretary of Defense, Policy for Department of Defense (DOD) Interactive Internet Activities, 8 June 2007.
- i. 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.
- j. AR 27-60, Intellectual Property, 1 June 1993.

I. Introduction

This legal opinion addresses the myriad legal issues associated with commercially hosted and provided social media use by Army personnel. Social media is defined herein as a set of commercial (not hosted or provided by the Department of Defense), Internet-based, participatory technologies, tools and platforms facilitating the creating, discovering, releasing, sharing, exchanging, and discussing of information, including user generated content.

There are two general functional areas of social media that potentially contribute to the defense missions. These are: (1) Internal Collaboration – Information sharing within agencies; and (2) External Communication – Information sharing with entities or parties external to federal agencies. Within this last functional area, there are two distinct components: (a) Outbound Information sharing, having the purpose to communicate with the public through posting official content and official branding; and (b) Inbound Information sharing, having the purpose of obtaining input and opinions from members of the public. The remaining discussion focuses primarily on the use of social media for external communications with the public.

II. General Policy

There are two types of social media accounts: personal accounts and Agency authorized accounts. Agency authorized accounts may be used for individual and/or organizational communication.

SAGC

Subject: Use of Social Media in the Army

Personal accounts:

Personal accounts may be established by an agency employee in his or her personal capacity. Such accounts must have no connection to official agency sites and must not appear to be, or represent, official opinion or content. Personal account pages should display a disclaimer that it is not an official page or communication nor does it express official DoD/DA positions. Personal accounts cannot be established with government email addresses, and cannot be used to conduct official business, or release official agency information, or for any other official communication related to the employee's government job or activities. Lastly, agency personnel having a personal social media account must comply with the Joint Ethics Regulation, and the Standards of Ethical Conduct for Employees of the Executive Branch, (see: 5 CFR Part 2635). These rules include prohibition on releasing non-public information, require appropriate disclaimers of opinions being expressed, and restrict the use of government computers to access and manage personal pages or communications during official duty time.

Authorized Accounts:

Agency authorized accounts can only be established under proper authorization from the Agency Head, or the delegated official. All vendor hosting services selection and Agency page or presence must comply with appropriate law, regulation, and policy, and must not compromise data confidentiality or integrity or release non-public information. Content on these pages or Agency presence must not contain political or discriminatory content, and not endorse or appear to endorse or show favoritism to nonfederal entities. Content or views must reflect U.S. Government policy and may not appear to endorse views contrary to U.S. Government policy. Those authorized to establish an Agency authorized account and organizational presence in electronic social media must receive training on the scope and authorized uses of social media, and ensure Public Affairs, Privacy, and OPSEC review of content before release or disclosure.

All pages or communications, or other means of organizational presence in social media must, to the extent technically feasible, display the required notices and disclaimers, identified herein, and unless expressly authorized by regulation, must not be represented as the "official" agency site or homepage. Additionally, two-way communications conducted for public affairs activities or for programs or actions that shape emotions, motives, reasoning, or behaviors of selected foreign entities falls within the scope of the Deputy Secretary of Defense Memorandum, "Policy for Department of Defense Interactive Internet Activities," June 8, 2007.

III. Process To Establish Agency Authorized Social Media Accounts and Presence

Authority & Acceptable Clauses

The Agency Head or delegated agency official may authorize agency employees to establish individual and organizational presence in social media necessary to the defense mission of the agency or organization. No individual and organizational presence should be

SAGC

Subject: Use of Social Media in the Army

established without, or prior to, official authorization. Common missions with obvious justifications suitable for a social media presence are Public Affairs and Recruiting. There may be others, as limited by the ability to articulate or justify an official purpose associated with the agency's mission or area of responsibility. Persons authorized to establish social media presence should be given express authorization in written form to make a record of the justification and authorization.

Because some social media hosting services have terms and conditions of use that the Federal government cannot legally accept, only those social media services that have specifically agreed to "Federally acceptable" terms and conditions or clauses can be authorized. The agency will need to identify those permissible hosting services. Authorized presence in commercial social media must be expressly tied to the acceptable/approved terms and conditions of use.

CIO Waivers

Authorized presence in commercial social media, like an agency Face-book page, for example, are subject to DoD and Army policies for Web sites and DoD information. AR 25-1 provides that "only official Army information that is releasable and of value to the public may be posted on Army public Web sites." Hence, unless provided for by other express regulatory authority, these authorized uses of social media are regulated by the same guidance as all other official websites on ".mil" domains, and must obtain a waiver of the ".mil hosting" requirements from the Army CIO/G-6. Additionally, AR 25-1 provides a list of information which Army public websites will not publish/post, including FOIA-exempt information. Recommend the CIO/G-6 establish clear and rapid procedures for processing these social media waiver requests.

IA Security Risk Assessments & Information Collection

Some commercial social media hosting services may pose information assurance (IA) security risks, or violate law or policy for a Federal entity on the collection of information from the public via multisession cookies or other means that track user's identification and internet activity across several sites. Recommend that the CIO/G-6 establish a listing of social media services that are relatively IA safe, or susceptible to risk mitigation, and do not violate Federal or agency rules on collecting information from the public. Authorized services should be restricted to only those validated by the CIO/G-6.

Training & Education of Users and Presence Managers

Agency employee presence managers of approved social media services should receive prior training and education on the scope and authorized use of the services. Training should address the limitations on content that can be disseminated via these services; ethical use and endorsement issues; prohibitions on partisan political activities and discriminatory content, events, or groups; content review for security (OPSEC), privacy, and public affairs purposes;

SAGC

Subject: Use of Social Media in the Army

and regulatory listed prohibited content. To the extent it has not done so already, the Agency should develop training materials in this area.

Selection of Host Providers

While there may not be a cost to the Agency associated with establishing authorized presence in social media, these are commercial hosting social media services, generally in business to make a profit, usually through advertising. Consequently, the Agency must select the hosting services on a fair and reasonable basis, subject to the Agency requirements associated with the mission objectives supporting the decision to establish a social media presence, and consistent with IA security concerns, and limited to consideration of hosting services with acceptable terms and conditions. Since these services stand to reap financial gain from the Agency bringing users/viewers to their commercial sites, it is important that the Agency or organization concerned develop standards and parameters of its requirements and then select the most suitable services provider(s) that meet the security concerns, and have acceptable terms and conditions. Select a provider based on the Agency requirements, security concerns, demographics, market share, and Agency resources and acceptable terms and conditions. This is necessary to avoid appearance of endorsement and favoritism – and possible protest litigation. This process can be done similar to an acquisition market research selection process.

IV. Content

Content Review: OPSEC, Public Affairs, and Privacy Interests

Prior to release, disclosure, or posting of information on the public social media presence, the content must be reviewed by properly trained persons for a variety of purposes. DoD Directive 5230.09, Clearance of DoD Information for Public Release, provides that "any official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the Department of Defense shall be reviewed for clearance prior to release." Content or views must reflect U.S. Government policy and may not appear to endorse views contrary to U.S. Government policy. Public affairs offices shall conduct this review in accordance with regulations specified in DoDD 5230.09 Enclosure I, References. Joint Ethics Regulation (JER) 3-211, Requirements for Public Speakers in an Official Capacity, provides that public presentations must serve DoD public affairs interest, military training interests, or community relations interests. JER 3-211 also requires that any presentation event or context must be appropriate for association with DoD and not be prohibited by statute or regulation.

Prohibited Information.

Any official information that is generally not available to the public and which would not be released under the Freedom of Information Act (FOIA) cannot be posted to a social media presence. Examples include but are not limited to:

SAGC

Subject: Use of Social Media in the Army

- (1) Classified information.
- (2) Casualty information before the next-of-kin has been formally notified by the Military Service concerned.
- (3) Information protected by the Privacy Act.
- (4) Information regarding incidents undergoing investigation.
- (5) Information considered Essential Elements of Friendly Information (EEFI).
- (6) For Official Use Only information.
- (7) Information identified on the current Critical Information List.

Records Management

Authorized social media presence content is not excluded from records management requirements simply because it is located outside the ".mil domain". The Agency is legally obligated to create and maintain adequate and proper documentation of its organization, functions, and activities. Recordkeeping requirements are embodied in laws, regulations, and Agency directives providing general and specific guidance on particular records to be created and maintained by an Agency. Any electronic information generated by or contained in an information system (IS) or other automation source, created or received during the conduct of business, must be preserved according to those instructions (or if unscheduled, as established by the site Records Manager).

Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved, or appropriate for preservation, by that Agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them. Electronic records include numeric, graphic, and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record.

The Federal Records Act of 1950, (FRA), 44 U.S.C. § 3301, et seq., as amended, contains the statutory authority for the Army Records Information Management System (ARIMS) program. Army records, regardless of medium, must follow the disposition instructions identified in ARIMS RRS-A and comply with the security requirements of AR 25-2. Any electronic information generated by or contained in an information system (IS) or other automation source, created or received during the conduct of business, must be preserved according to those instructions (or if unscheduled, as established by the activity records manager). Army

SAGC

Subject: Use of Social Media in the Army

Regulation (AR) 25-400-2 governs the maintenance and disposition of Army information and provides policy on managing information from its creation through final disposition according to Federal laws and Army recordkeeping requirements.

Recommend the Army publish specific records management guidance for official social media presence content, especially addressing preservation and disposal. Until then, persons establishing authorized a social media presence should consult with the applicable activity records manager and their legal advisor.

Collection of Information from the Public & Moderation of Public Comment

One of the uses of a social media presence is inbound sharing - to more easily obtain input from members of the public, and to obtain personal comments on issues in real time on current topics of interest. There are, however, legal restrictions on the collection of information from the public. The Paperwork Reduction Act of 1995 requires government agencies to seek and obtain approval from the Office of Management and Budget (OMB) prior to obtaining or soliciting "identical" information from 10 or more persons. The approval process, which is popularly known as the "OMB clearance process," is extensive and time-consuming. It requires two Federal Register notices and a detailed application to OMB. The duration for the entire process can exceed six months. Consequently, social media presence managers must be cautious in any attempt to solicit information from the public in a structured manner. A presence manager should obtain legal advice prior to conducting any type of public poll or survey for information on the social media presence.

There are additional rules that may apply to any Agency authorized social media presence that will collect personal information from users that will access the presence. Any such collection of information regarding students may have to comply with 10 USC § 503 – Recruiting campaigns and compilation of directory information. For recruiting efforts, under that statute, collection of information from public persons (students etc.,) must be from persons 17 years or older, the use of the information is limited for recruiting only, and the information must be disposed of after three (3) years of collection. More generally, compliance with the Privacy Act is required for any personal information collected and maintained and retrievable in a system of records. This could require Privacy Act Statement at time of collection, a System of Records Notice (SORN) which identifies the system of records and is published in the federal register, safeguarding of the data in accordance with DoDD 5400.11 DoD Privacy Program, and notice to the individual if the personal data is lost or compromised. In accordance with the requirements of the Privacy Act in regard to this type of collection into a system of records, the collected data, and user logs, should not be stored on the commercial server, as that may constitute a disclosure.

SAGC

Subject: Use of Social Media in the Army

Moderation of Public Comments

For those social media presence like Face-book that "accept" friends or that will have blogs or other means for the public to post comments on the Agency presence, there will need to be a periodic review of comments and screening of those who "sign up" as "friends" or such a similar concept. This is necessary to avoid association with offensive or messages/groups who are considered inappropriate for association with DoD.

Public comments will need to be screened to remove information inappropriate for association with DoD posted by public "friends" which do not comply with DoD and Federal policies applicable to websites.

Presence managers will need to delist persons/entities previously accepted as a "friend" who post inappropriate content or are found to be unacceptable for association with DoD.

A proper disclaimer addressing these matters should also be posted on the presence. In the case of a Face-book page, this disclaimer will need to be reposted periodically to the Agency Face-book "Wall" to ensure the disclaimer does not drop off or get lost in chronologically organized postings.

Linking to Other Pages, Sites, and Disclaimers

In accordance with AR 25-1, paragraph 6-7(c)(7), Army commands and activities will establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Web sites. This requirement would apply to authorized social media presence. Guidelines should consider the information needs of mission-related requirements and public communications and community relations objectives. No compensation of any kind may be accepted in exchange for a link placed on an organization's publicly accessible authorized social media presence. Listings of Web links on Army social media presences should separate, where feasible, external Web links from Government and military links. When external links to non-Government Web sites are included, a suitable disclaimer should appear or be displayed to the extent technically feasible.

Copyrights, Trademarks and Licensing

Copyrights

Authorized social media presence must comply with Federal copyright laws and Agency regulations. The recording, duplicating, and/or use of copyrighted material on an authorized social media presence is prohibited by law (17 USC §106) unless prior authorization from the copyright holder is obtained in writing. The use of copyrighted material by the Army is subject to U.S. Copyright Law as reflected in Army regulations. It is Army policy to recognize and respect the rights of copyright owners. In addition, any use of copyrighted material, for which

SAGC

Subject: Use of Social Media in the Army

permission has been obtained, will carry attribution for the source of the material. Copyrighted material in the Army's possession should be safeguarded from accidental unauthorized release. No copyrighted or otherwise proprietary content, photographs, or original works will be posted without written permission from the rightsholder. Photographs from embedded reporters are copyrighted and cannot be publically distributed without written authorization from the reporters.

A copy of the license or permission must be handled in accordance with Army records retention regulations and AR 27-60, Intellectual Property, paragraph 1-7U and Chapter 4.

Trademarks

The Army uses a wide variety of words, phrases, insignia, logos, and similar identifiers as marks to identify itself, its programs, services, and products. In all cases, marks are used to prevent unwanted or unauthorized exploitation of the good will obtained by the Army through the use of DA-owned marks. The terms "trademark" and "mark" include trademarks, service marks, collective membership marks, and certification marks used by the Army, whether or not a mark is registered under state or federal law. The many symbols, names, insignia, and logos of the Army represent the time-honored qualities of the Army's service to the Nation. They operate as legally-recognized marks, and are invested with goodwill deserving of protection.

Trademark Licensing

The Army may license its marks commercially and retain and expend the fees received from such licensing in manners consistent with federal law, DoD regulations, and AR 27-60. The licensing of these marks can bring credit to the Army and its Soldiers and help communicate the Army's values to the public at large.

Social media presence managers must not post Army or DoD trademarks on the public presence without prior approval from the Regulatory Law and Intellectual Property Division, U.S. Army Legal Services Agency (USALSA).

Section 508 Compliance

Under current statutory requirements, Federal Agency public web pages are required to comply with the provisions of Section 508 of the Rehabilitation Act Amendments of 1998 (29 U.S.C. § 794d). Public web pages must be equally accessible to disabled and non-disabled Federal employees and members of the public. Guidance on Section 508 standards concerning Web-based information and applications is located at <http://www.access-board.gov/sec508/508standards.htm>. Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals. Authorized Agency content uploaded to these commercial social media sites may be subject to Section 508 compliance requirements – unless an exception applies.

SAGC

Subject: Use of Social Media in the Army

One exception to the compliance requirement is a showing of an undue burden. Undue burden is defined as a “significant difficulty or expense.” In determining whether an action would result in an undue burden, an Agency shall consider all Agency resources available to the program or component for which the product is being developed, procured, maintained, or used.

Section 508 also provides that if a Federal Agency determines that compliance with the standards in procurements imposes an undue burden, any documentation by the Agency supporting procurement shall explain why compliance creates an undue burden. In determining whether compliance with all or part of the applicable accessibility standards in 36 CFR § 1194 would be an undue burden, the requiring officials must consider the difficulty or expense of compliance, and all Agency resources available to its program or component for which the supply or service is being acquired.

In the case of an authorized social media presence on a commercially hosted webpage, an undue burden analysis could determine that the Agency lacks sufficient control over this activity. The analysis could focus on the point that much of the content is available on the Agency’s official web page; public provided comments are constantly changing and difficult to capture; and more significantly, the content is on a commercial hosting service not under the control or direction of the Agency, and not otherwise required to comply with section 508. Any such undue burden analysis should be done and properly documented before the official social media presence opens to the public.

V. Disclaimers & Notices

Agency regulations and policy require several disclaimers and notices to be displayed on official Agency web pages, which include any authorized social media presence, even those hosted on commercial domains. Such disclaimers include a general disclaimer, privacy and security disclaimer, copyright and trademark disclaimer, Persistent Cookie disclaimer, External links and Endorsement disclaimer, Moderated presence disclaimer – if public content can be displayed or uploaded to the presence, and a FOIA and Records Management Notice. Disclaimers or Notices required by Army regulations are controlling. Based on the structure of some social media hosting services - disclaimers and notices may need to be reposted periodically to the Agency presence to ensure the disclaimer language do not drop off or get lost in chronologically organized postings.

The following sample Disclaimers and Notices are provided for review and consideration, and may need some adjustment before adoption.

General Disclaimer

The purpose of this social medial presence for the [COMMAND/ORGANIZATION] is to keep the American people and the U.S. Army informed, and helps to establish the conditions that lead to confidence in America's Army and its readiness to conduct operations in peacetime,

SAGC

Subject: Use of Social Media in the Army

conflict, and war. Through its websites and other online resources, the Army offers broad public access to a wide range of information. This presence complies with appropriate law, regulation, and policy. Content on this presence may not contain political or discriminatory content, and will not endorse or appear to endorse or show favoritism to nonfederal entities.

Privacy & Security

The [presence] is provided as a public service by [ORGANIZATION/COMMAND] in coordination with Army Public Affairs. Information presented on [presence] is considered public information and may be distributed or copied unless otherwise specified. Use of appropriate byline/photo/image credits is requested.

This page is hosted on a non-DoD hosting service provider as a social media presence for the [COMMAND/ORGANIZATION] and is not subject to the control or direction of the U.S. Army for purposes of site management, compliance with Section 508 of the Rehabilitation Act, or the collection of information on those persons who may view this presence. For more information see the Privacy Terms & Conditions for the hosting service provider for this presence.

Use of Copyrighted Material

The use of copyrighted material by the Army is subject to U.S. Copyright Law as reflected in Army regulations. It is Army policy to recognize and respect the rights of copyright owners. Army Regulation 25-1 prohibits the posting of documents or information protected by copyright on Army websites without the written permission of the copyright holder. Permission to copy a video, photo, graphic, or other material protected under U.S. Copyright Law on this webpage must be obtained from the original source. Please note that many photos and materials used on this presence and produced by the U.S. Army may not be protected under U.S. Copyright Law. Given the presence of works with different levels of protection on this presence, do not upload any copyrighted materials without prior written permission of the copyright holder. This presence does not create any right, remedy, or cause of action for any person against the Army.

Unauthorized attempts to upload information or change information on this presence are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

Cookie Disclaimer

The Army does not use persistent cookies (persistent tokens that pass information back and forth from the client machine to the server). However, the hosting service provider on which this presence is hosted might use persistent cookies, depending on the policies applicable for the hosting service provider. The Department of Army DOES NOT keep a database of information obtained from these cookies, if any. The hosting service provider might allow you to

SAGC

Subject: Use of Social Media in the Army

choose not to accept these cookies and still access or use the site. You should read the Terms & Conditions for the hosting service provider for more information. Refer to the help information in your browser software for instructions on how to disable cookies.

External Links & Non-Endorsement Disclaimer

The appearance of advertisements or hyperlinks to external sites does not constitute endorsement by the U.S. Department of Defense or the U.S. Army of the linked web sites or the information, products or services contained therein. The U.S. Army does not exercise any editorial control over the information you find at these locations. Such links are provided consistent with the stated purpose of this Army Web presence. Please let us know about existing external links which you believe are inappropriate and about specific additional external links which you believe ought to be included.

DoD, the Army, and the [COMMAND/ORGANIZATION] does not endorse either the hosting service provider, advertisers of the hosting service provider or any poster, friend, or message from a non-DoD entity who posts to the [COMMAND/ORGANIZATION] presence. The Army does not advocate purchasing any item associated with hosting service provider or advertised on the hosting service provider's site, nor advocate donating or providing resources to any advertiser associated with the hosting service provider.

The Army does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained on a linked website. The Army does not endorse the organizations sponsoring linked websites or the views they express or the products/services they offer. The Army cannot and does not authorize the use of copyrighted materials contained in linked websites. Users must request such authorization from the sponsor of the linked website. The Army is not responsible for transmissions or access to photos or videos users receive from linked websites. The Army does not guarantee that the non-DoD hosting service provider, which hosts this Army presence or any linked external websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

Blog Comment Policy:

The blog section of this presence does not represent official U.S. Army communications. Any publicly accessible blogs on this Army presence are moderated blogs. That means all comments will be reviewed before or soon after posting. In addition, we expect that participants will treat each other, as well as our Department and our employees, with respect. We will not post comments that contain vulgar or abusive language; personal attacks of any kind; or offensive terms that target specific ethnic or racial groups. We will not post comments that are spam, are clearly "off topic" or that promote services or products. Comments that make unsupported accusations will also not be posted.

Any references to commercial entities, products, services, or other nongovernmental organizations or individuals that remain on the presence are provided solely for the information of individuals using this blog. These references are not intended to reflect the opinion of the

SAGC

Subject: Use of Social Media in the Army

Department of Defense, the U.S. Army, or its officers or employees concerning the significance, priority, or importance to be given the referenced entity, product, service, or organization. Such references are not an official or personal endorsement of any product, person, or service, and may not be quoted or reproduced for the purpose of stating or implying DoD/DA endorsement or approval of any product, person, or service.

Only comments that comply with this blog use policy will be approved for posting. The use of vulgar, offensive, threatening, or harassing language is prohibited. Blog public comments should be limited to comments related to the posted topic. The blog is not the proper place to express opinions or beliefs not directly related to that topic. The blog is not open to comments promoting or opposing any person campaigning for election to a political office or promoting or opposing any ballot proposition. The blog is not open to the promotion or advertisement of a business or commercial transaction. Communications made through the blog's e-mail and messaging system {if any} - will in no way constitute a legal or official notice or comment to the Department of Defense or any official or employee of the U.S. Army for any purpose. This blog use policy is subject to amendment or modification at any time to ensure its continued use is consistent with its intended purpose as a limited forum.

Security Risks to the DoD Network

Using social media to communicate with the general public can in some instances enhance the Army's ability to disseminate public information, increase recruiting, and effectively manage the Army's public image. As noted previously, there are risks inherent in using DoD computers to access social media/social networking sites. The Joint Task Force – Global Network Operations (JTF-GNO) recently noted that social networking sites can pose a significant hazard to network security, personal privacy, and in extreme cases, personal safety. JTF-GNO further noted that social networking sites continue to be vectors for injecting malicious codes, and social engineering to reveal sensitive information. The decision to authorize an Agency social media presence should take into consideration the considerable risks posed by exposing DoD computers to social media or social networking sites.



Jeffrey L. Caddell
ASSOCIATE DEPUTY GENERAL COUNSEL
(ACQUISITION, INFORMATION TECHNOLOGY & BIOMETRICS)